PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 29/06, 12/22

A1

(11) International Publication Number: **WO 00/52900**

(43) International Publication Date: 8 September 2000 (08.09.00)

(21) International Application Number: PCT/GB00/00748

(22) International Filing Date: 2 March 2000 (02.03.00)

(30) Priority Data:
9904791.2 2 March 1999 (02.03.99) GB

(71) Applicant: OBONGO LIMITED [GB/GB]; Elsley House, 24–30 Great Titchfield Street, London W1P 7AD (GB).

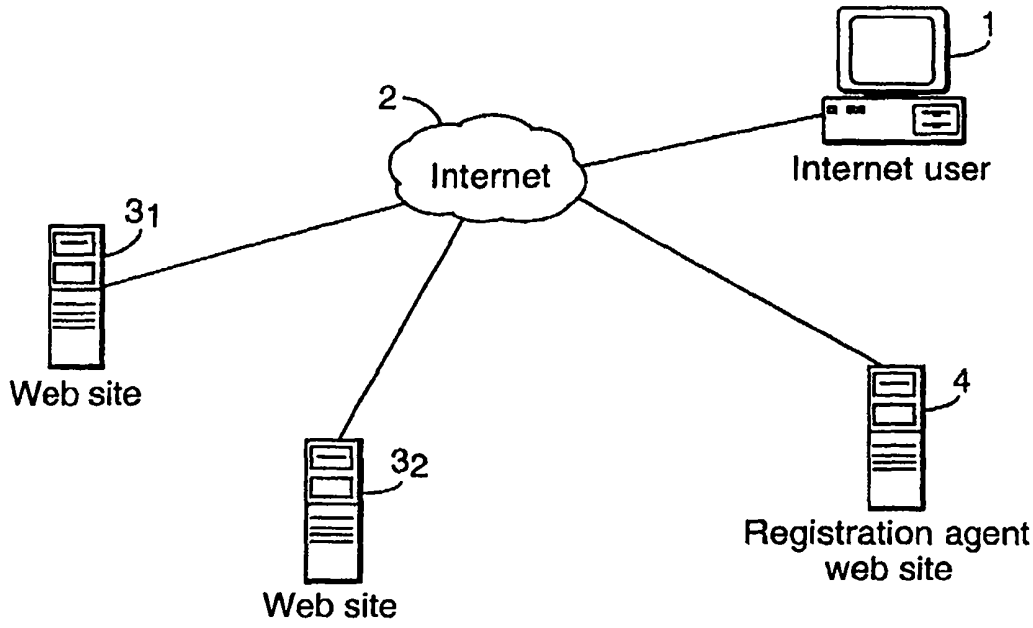
(72) Inventors: HUNT, John; Obongo Inc., 955 Charter Street, Redwood City, CA 94603 (GB). GLADSTONE, Ben; Obongo Inc., 955 Charter Street, Redwood City, CA 94063 (US). MORRIS, Kief; Obongo Inc., 955 Charter Street, Redwood City, CA 94063 (US). KALAHER, Patrick; Obongo Inc., 955 Charter Street, Redwood City, CA 94063 (US). BYRN, Mark; Obongo Inc., 955 Charter Street, Redwood City, CA 94063 (US). MOILANEN, Esa; Obongo Inc., 955 Charter Street, Redwood City, CA 94063 (US). LIDWELL, Peter; Obongo Inc., 955 Charter Street, Redwood City, CA 94063 (US).

(74) Agent: ELKINGTON AND FIFE; Prospect House, 8 Pembroke Road, Sevenoaks, Kent TN13 1XR (GB).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: AN INTERNET INTERFACE SYSTEM



(57) Abstract

The present invention provides a registration agent site (4) which presents a simple intermediary between sites (3) and internet users (1) that acts a single source of data entry, user name and password for users. This allows users to register with new sites automatically and move between registered sites via a single interface, whilst allowing changes in profile information via the same interface. The registration agent site (4) acts as the agent for the internet user (1) rather than the site owner, allowing registration by proxy in a manner which is transparent to other sites. The agent negotiates connectivity and connects the user.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

AN INTERNET INTERFACE SYSTEM

Field of the Invention

The present invention relates to the registration of internet users at websites.

Background to the Invention

Before using many websites, internet users need to fill in an often cumbersome registration form providing personal data. Site owners require this information for marketing purposes and to personalise the offering to customers. Registration demands can range from the basic requirement of a name and email address to a detailed request for personal information including street address, employment details and even salary levels. This process gives rise to a number of problems for users. Registration is often slow and not intuitive, with an additional problem that formats differ from site to site. Once registered with more than one site, users also have the problem of keeping track of the different user names and passwords that they use. When a user's information changes (email, addresses etc.) the management of multiple registrations becomes unwieldy. Furthermore, users have little or no control of information released to sites which can on-sell the personal data leading to both a breach of individual privacy and, perhaps inevitably, an accompanying barrage of unwanted direct marketing emails or "spam".

A typical internet user may be registered with between four and ten sites and would probably register with one new site each month. The greater these numbers the more serious the problem becomes. New users and sites are coming to the internet at exponential rates of growth so this problem can only get worse.

Though necessary for their business model, registration also poses a major problem to site owners. Users quite often enter bogus information (often several times having forgotten their password and thus having to register anew), which is of no use to site owners whilst bearing a data storage cost. Bogus information is entered for a number of reasons: frustration with the speed of the registration process, a general mistrust of the security and subsequent use of the data, or simply because the user has forgotten the previous registration details. Indeed, as much as 50% of all consumer data held by major sites on the internet is estimated to be false. Even genuine registration data becomes inaccurate over time if it is not up-dated.

Another problem is that users frustrated with the registration process will stop before completion so that the site loses a new potential customer. It is estimated that over 50% of potential users are lost due to aborted registrations.

Summary of the Invention

According to a first aspect of the present invention, in an arrangement comprising at least one computer network connecting at least one personal computer to at least one service computer, the personal computer being associated with at least one user, a method for managing the registration of the user with the at least one service computer, the method comprising the steps of:

gathering registration data for the at least one service computer;

storing the registration data in at least one data structure on at least one registration agent computer connected to the computer network;

gathering personal data for the user;

storing at least part of the personal data in at least one data structure on at least one registration agent computer connected to the computer network; and,

in response to a request from the user to a registration agent computer connected to the computer network to register the user with the at least one service computer, submitting an application to register the user with the at least one service computer by transmitting registration information from at least one registration agent computer to the service computer, the registration information being compiled from data obtained by accessing the users personal data stored in the associated data structure and by accessing registration data for the service computer stored in the associated data structure.

The service computer may be a product-provider and/or an information-provider.

According to a second aspect of the present invention, in a method for registering a user at a client node of a communications network with at least one server node connected to the communications network by the use of at least one registration agent server node connected to the communications network which stores personal data associated with the user together with registration data associated with the at least one server node, the method comprising the steps of registering the user with the at least one server node in response to a user request received at the registration agent server node by completing and transmitting on behalf of the user a registration application from the registration agent server node to the at least one server node based on the personal data associated with the user and the registration data associated with the at least one server node.

Preferably, the computer or communications network utilises an internet protocol.

Preferably, each of the service computer or server nodes is a website having a server connected to an internet or intranet. Preferably, the at least one registration agent computer or registration agent server node is connected to an internet, intranet or internet protocol (IP) network.

Preferably, the at least one registration agent computer or registration agent server node is a World Wide Web server.

Preferably, the at least one registration agent computer or registration agent server node operates a World Wide Web site.

Preferably, the step of transmitting an application to register the user is preceded by the step of verifying a user identification and more preferably, a password, entered by the user which identifies the user with respect to the associated personal data.

Preferably, the method includes the steps of storing personal data in the form of a master user profile data structure which uniquely describes the user, together with a number of personal registration data structures, each of which describes registration data associated with the successful registration of the user with a service computer or server node. The personal registration data structures permit repeat visits to the service computer or server node without the user having to go through the registration procedure again.

Preferably, the method includes the step of accepting user inputs which define a privacy policy in relation to the user's personal data which describes the extent to which the personal data is to be released for the purpose of submitting a registration application.

Preferably, the method includes the step of providing a unique proxy address for the user in a registration application so that communications addressed to the user using the unique address are received by the at least one registration agent computer or registration agent server and are subsequently forwarded to the user. More preferably, the communications are forwarded to the user in dependence on an email filtering policy accepted by the user. Most preferably, a different proxy address for the user is allocated for each subsequent registration with other service computers or server nodes.

According to a third aspect of the present invention, an apparatus for managing the registration of a user in accordance with either one of the first and second aspects of the present invention, comprises:

means for storing registration data;

means for storing personal data;

means for receiving a user request to submit a registration application on behalf of the user to a remote site;

means for completing a registration application based on a combination of personal data associated with the user and registration data associated with the remote site; and,

means for transmitting a completed registration application to the remote site on behalf of the user.

Preferably, the apparatus comprises a computer storage medium containing computer executable instructions for performing the method of either one of the first and second aspects of the present invention. More preferably, the apparatus comprises a server.

Most preferably, the server is arranged to provide a website having a unique resource locator (URL).

In one example, the present invention provides a registration agent site which presents a simple intermediary between sites and internet users that acts a single source of data entry, user name and password for users. This allows users to register with new sites automatically and move between registered sites via a single interface, whilst allowing changes in profile information via the same interface. The registration agent site acts as the agent for the internet user rather than the site owner, allowing registration by proxy in a manner which is transparent to other sites. The agent negotiates connectivity and connects the user.

In terms of the internet user, the benefits of using the interface provided by the registration agent site can be summarised as follows: the interface provides a convenient way of navigating between sites since it is necessary to remember only one password; the interface provides an effortless way of registering with new sites; it offers the ability to effect a global change across sites; it provides for the control of privacy by allowing the user to define a privacy policy; and, it allows for the integration of email filtering by proxy to prevent "spamming".

The registration agent site provides a central repository of all personal information that an individual internet user is, at least to some extent, prepared to give out to sites in order to register with the site. Personal details particular to each site registration are stored as well as a master profile of all personal information. This information can be recalled and modified via the interface. Accordingly, the user of the interface will know what personal information has been given out and to whom as well as the

totality of information given out to all sites. Users are able to impose specific controls on how their personal information is used to register with a site including the complete prohibition of the use of certain information, provided this does not conflict with a site's registration requirements. If there is a conflict, the interface allows this to be resolved by deferring to the user for a final decision.

In summary, the service that the interface of the registration agent site provides is one of assisting internet users to complete registration forms for websites by proxy, and logging into their sites on repeat visits. The user does not have to retype information, can have different profiles, can automatically check privacy policies, can review what data has been given out and to whom, and can protect their email address. Indeed, a key component of helping users control their interaction with sites is to protect their email address from being abused by the sites they give it to. The present invention offers the option to give protected email addresses to sites when a user registers through the interface. The site does not receive the users real address, but is instead given a unique proxy address (a different one for each site). Email sent to that address is forwarded to the users email account. This allows users to selectively cut "spammers" off without having to change their email address. It also allows users to identify which sites are giving their email addresses to third parties which use it for "spam".

Brief Description of the Drawings

An example of the present invention will now be described in detail with reference to the accompanying drawings, in which:

Figure 1 is a simplified schematic diagram showing an internet user's computer connected to the World Wide Web;

Figure 2 is a simplified block diagram of an example of a registration agent website server;

Figures 3 and 4 show an example of an internet user registering with a website; and,

Figures 5 and 6 show an example of an internet user transferring registration information for a number of websites to a registration agent website.

Detailed Description

Figure 1 is a simplified schematic diagram showing an internet user's computer 1 connected to the World Wide Web 2. The internet user's computer 1 uses web browsers to navigate the World Wide Web to access desired services, known as websites 3. Many websites require an internet user to register at the website, wherein the user is required to establish a user identification and optionally a password for the website. Typically, the user is also asked to provide other personal information, not all of which is mandatory. The present invention provides a registration agent site (RAS) 4, in this example a web server, which presents a simple intermediary between sites and internet users that acts as a single source of data entry, username and password for users. The invention allows users to register with new sites automatically and move

between registered sites via a single interface, whilst allowing changes in profile information via the same interface. The interface acts as the agent for the internet user rather than the site owner, allowing registration by proxy.

Figure 2 is a simplified block diagram of an example of a registration agent site 10. The web server includes a registration processing system 11 which controls the steps of lodging a registration with websites on behalf of internet users who are registered members of the registration agent site. The server stores user profiles in a user database 12 which represent a master profile of all personal information, including a privacy policy, and personal details particular to each website where the user has registered to date. Each website that is affiliated with the registration agent site is represented in a registration profile database 13 where details of the site registration requirements, including the registration forms used by the website, are stored.

The core service provided by the registration agent site 10 is one of assisting users to fill out forms on websites, primarily targeted towards registering with new sites and logging into sites on repeat visits. The user does not have to retype information, can have different profiles, can automatically check privacy policies, can review what data they gave out and to whom, and can protect their email address. The system does not require any plug-ins or software downloads, and is browser independent.

The registration processing system 11 is responsible for submitting user data to a site's registration system. This involves the following functionality:

1. analysing the site's data requirements and forms handling system (in other words, what data do they want from the user and how does their registration system work?);

2. determining the site's data privacy policies;

3. marshalling the appropriate user data;

4. identifying and resolving conflicts between the user's privacy preferences and the site's policies;

5. providing the data to the sites; and,

6. storing information about the transaction.

The functionality and data requirements can be divided into three sections: interfacing with target sites, managing and using data, and interfacing with the users.

When a user wants to fill out a form on a site, the registration agent site 10 must marshal the appropriate user data and provide it to the target site. This implies two core parts of the interface: determining what data the site needs and supplying the data to the site.

A simple way to supply data to sites is to submit it directly to the site's own forms processing applications in the format it expects it. This involves making an HTTP GET or POST request to the uniform resource indicator (URI) to which the site's own HTML forms submit their data. Alternatives include using JavaScript to fill the site's form or proxying form submission. In the latter, the registration processing system acts as an HTTP client, connects to the target site's webserver and submits the form. Moreover, preferably, the registration processing system 11 uses a process which emulates the normal registration by a user by providing a form which duplicates the data submission of the site's own form. The registration processing system 11 generates an HTML page which is dynamic and which contains a form with all of the

relevant data fields of the site's own form. The target for this form submission is the same URI which the site's form submits to.

Any system for submitting data to a site on behalf of a user will need certain information about the site and its form system, which is termed Site Data Requirements (SDR). A given site's SDR is stored in the registration profile database 13, and needs to include at least some of the following information:

1. what forms are on the site?

2. what are the site's data privacy policies? Is there any relevant third party auditing or accreditation?

3. for each form, what URI is the form submitted to?

4. for each form, what data fields are needed?

5. for each data field, is the data contained in the user profile, and if so, which field of the profile?

6. for each data field, if the data is not contained in the user file, what description should be shown to the user to explain what is needed?

7. for each data field, what values are acceptable as input? This includes whether the field is required or optional;

8. for each data field, what name is it given by the site's forms processing system? and,

9. for each data field, is the user's data going to be unique to this site, for example user name and password, as opposed to something which can be the same on all sites, such as postal code?

SDRs can be determined in a number of ways. In one example, an individual must first analyse the sites to determine the requirements and enter the information into the registration profile database 13. It would then be possible to update the stored data to take account of any changes which subsequently occur. This update may be implemented automatically. In another example, it may be possible to interrogate the site automatically in an intelligent fashion to determine the SDR. Affiliated sites may also cooperate by embedding encoded information into their HTML forms to allow the SDRs to be determined automatically by the registration processing system.

The user profile database 12 stores a collection of data for each user. A user is able to view all data maintained about them as an individual and normally no one else has access to this without the express permission of the user.

The user profile file structure includes personal preferences data which is used as part of the interaction with the registration agent site and includes the user name and password, as well as information for customisation of the user interface. This information is not available to sites.

The user profile file structure also includes privacy preferences data which describe the policies the user would like a site to have if their data is to be given to the site by the registration agent site. This covers general policies for the site, whether or not the site's policies are certified, and also links policy choices to individual fields of the user personal data (described below). This linking allows users to specify that some data is more sensitive than others, so a site which only asks for low sensitivity data is not expected to have as rigorous a data privacy policy as a site which wants more sensitive data.

As mentioned above, the user profile file structure also includes personal data which is available to sites the user chooses to register with (although the data is still subject to the privacy settings described above). The registration agent site 10 stores a core profile which is a set of data fields required by more than one site. Users can have more than one set of core profile data which allows them to maintain a set of different "personalities", for example one for a work address and one for a home address.

Other personal data can be stored in site-specific user profiles forming part of the user profile file structure. These may consist of data which the user has supplied to a particular site, but which is not used for other sites. Examples include a user name and password for a site, or preference data specific to one site.

The registration processing system 11 also allows users the option to give "protected" email addresses to sites rather than their normal address. When a site requests the user's email address, the interface generates a new address in a mail domain and supplies that to the site. Email to the address is forwarded by the registration agent's system to the user's real email address, including a header indicating which site it originated from. Mail is not stored by the system, merely forwarded. The user can disable a protected address to prevent unwanted mail from reaching them.

The web server which supports the registration processing system and associated databases includes a server platform with appropriate hardware and an operating system, mail serving software, and a hosting service. The databases may be provided on the same machine or from a remote source which is networked to the web server.

A user can be introduced to the registration agent site 10 by navigating directly to the associated URL, from an affiliated site where they are registering for the first time

(they are presented with a registration button which provides a link to the registration agent site), or from an affiliated site where they are already registered (where again they are presented with a registration button). In the latter case, the user is prompted by the registration agent site 10 to provide their existing user name and password for the site either before or after registering with the registration agent.

When registering for the first time with the registration agent site 10, the user is presented with a form generated dynamically to gather the minimum information they need, given the circumstances. Core information required to sign up a new member includes the user's email address (which is subsequently verified). The new member chooses a username and password which is required on all subsequent visits to the registration agent site. If the new member is registering with a new site at this time, the user is presented with a form which sets out the information that the site will want for registration. The user is also presented with the option of filling out data fields required by most affiliated sites which will make signing up with new sites faster next time.

The information may be grouped into different categories, for example:

1. basic information (name, email address);
2. professional contact information (work address and phone number, etc);
3. personal contact information (home address, etc);
4. profession demographics (job title, etc); and,
5. personal demographics (size of family, hobbies, interests, dislikes, etc).

For each information group, the user chooses an information policy, which tells the registration agent site 10 when and to whom the information in that category can be given out. In this example, the choices are colour coded similar to traffic light colours. Green data is data that can be given out to any site the user wishes to register with. Yellow data can be given to a site which matches certain criteria the user sets. Red data will not be given out at all by the registration agent site, unless the user specifically agrees to it at the time the data is requested. The user can choose the circumstances under which the data they tag as yellow can be given to sites they register with. For example, the user may specify that the site must have certain data handling policies in place and perhaps that these policies must be verified by an independent agency.

As described above, there are a number of ways that an internet user can become a member of the registration agent site 10 and some examples of these will be described below. Throughout, the registration agent site and the interface it provides shall be referred to as "RAS".

In Figures 3 and 4, it is assumed that the internet user has navigated the World Wide Web using a web browser (step 100 or 200) to arrive at the login page of a website (referring site), of which they are not already a member, but which is affiliated with the RAS and provides a button or other icon with a URL to the RAS web server. The user is not already a member of the RAS. The user clicks on the RAS button appearing on the login page and a pop-up window appears and the browser window of the referring site goes behind. In step 101 or 201 the user completes the new member section of an entry page, giving a username, password, email address and language.

The user then selects an option that says that they are not already a member of the referring site and clicks on an "enter" button. A new page then appears in step 102 or 202 requesting additional information that is necessary for the user to actually register with the referring site. The site requirements are determined by accessing the registration profile database 13. A master user profile for the new member is created and stored in the user profile database 12, together with a personal profile for the new registration. Once the user has provided the additional information, they click "enter" and the user's new home page for the RAS appears (in step 203) showing the referring site as a registered site and a separate list suggesting other affiliated sites where the user may wish to register. The RAS pop-up window is then hidden behind the referring site window, which itself changes to the page showing that the user has successfully registered with the site.

In future, it is possible to logon to the same website by navigating directly to the RAS website (by typing the address for the registration agent site, assigning a bookmark or clicking on an advertisement banner), and then clicking on the listed entry for the site on the user's home page. Alternatively, the user can navigate directly to the website itself, click on the RAS button, and logon via the RAS website.

In each of the above cases, whether the procedure be a simple logon or a new registration, it is preferred that the process is entirely transparent to the website of interest in the sense that it is wholly unaware of the involvement of an intermediary.

In Figures 5 and 6, the internet user is already a member of both the RAS and a particular website (referring site). Again, the user is assumed to have navigated (in step 300 or 400) to the logon page of the referring site using their web browser, but is

seeking a more convenient way to sign in to the website. In step 301 or 401 the user clicks on the RAS button and a RAS pop-up window appears over the browser window of the referring site. The user enters their username and password for the RAS and selects the option that says that they are already a member of the referring site. The user then clicks "enter" and a new page appears with a request for the user's current login details for the referred site. In step 302 or 402 the user enters their current login details for the referring site and then clicks the "enter" button. The user's RAS home page then appears showing the referring site as a registered site (in step 403). A personal profile for this site is created and stored in the user's profile database 12 for future use.

In the example shown in Figure 6, the internet user decides to repeat the process in steps 405 and 406 for other sites which they are members of (but have registered with the sites independently of the RAS). The user switches back to the RAS window and on the home page enters the site name into a search box. The search results are displayed to the user in step 405 who then selects the appropriate site and the transfer of login details process is repeated as above in step 406.

An important aspect of the present invention is that it is possible for the user to specify a privacy policy (indicated in steps 103 and 104) which may restrict to some extent information the user is prepared to provide to sites in order to complete the site's registration forms. From knowledge of the registration requirements of each affiliated site (stored in the registration profile database), it is possible for the registration agent site 10 to determine whether or not a particular item of personal information is mandatory and subsequently warn a user that there is a policy clash before an attempt

to register with the site is made. A user can be given the option of making an exception in the circumstances or amending their global policy for the item of data in question.

In summary, the present invention provides a central repository of all personal information that an individual internet user is, at least to some extent, prepared to give out to sites in order to register with the site. Personal details particular to each site registration are stored as well as a master profile of all personal information. This information can be recalled and modified via the interface. Accordingly, the user of the interface will know what personal information has been given out and to whom as well as the totality of information given out to all sites. Users are able to impose specific controls on how their personal information is used to register with a site including the complete prohibition of the use of certain information, provided this does not conflict with a site's registration requirements. If there is a conflict, the interface allows this to be resolved by deferring to the user for a final decision.

CLAIMS

1. An arrangement comprising at least one computer network connecting at least one terminal to at least one service computer, the terminal being associated with at least one user, a method for managing the registration of the user with the at least one service computer, the method comprising the steps of:

gathering registration data for the at least one service computer;

storing the registration data in at least one data structure on at least one registration agent computer connected to the computer network;

gathering personal data for the user;

storing at least part of the personal data in at least one data structure on at least one registration agent computer connected to the computer network; and,

in response to a request from the user to a registration agent computer connected to the computer network to register the user with the at least one service computer, submitting an application to register the user with the at least one service computer by transmitting registration information from at least one registration agent computer to the service computer, the registration information being compiled from data obtained by accessing the user's personal data stored in the associated data structure and by accessing registration data for the service computer stored in the associated data structure.

2. A method for registering a user at a client node of a communications network with at least one server node connected to the communications network by the use of at least one registration agent server node connected to the communications network which stores personal data associated with the user together with registration data

associated with the at least one server node, the method comprising the steps of registering the user with the at least one server node in response to a user request received at the registration agent server node by completing and transmitting on behalf of the user a registration application from the registration agent server node to the at least one server node based on the personal data associated with the user and the registration data associated with the at least one server node.

3. A method according to claim 1 or 2, in which the computer or communications network utilises an internet protocol.

4. A method according to any preceding claim, in which each of the service computer or server nodes is a website having a server connected to the internet or an intranet.

5. A method according to any preceding claim, in which the at least one registration agent computer or registration agent server node is connected to the internet, an intranet or an IP network.

6. A method according to any preceding claim, in which the at least one registration agent computer or registration agent server node is a World Wide Web server.

7. A method according to claim 6, in which the at least one registration agent computer or registration agent server node operates a World Wide Web site.

8. A method according to any preceding claim, in which the step of transmitting an application to register the user is preceded by the step of verifying a user identification and more preferably, a password, entered by the user which identifies the user with respect to the associated personal data.

9. A method according to any preceding claim, including the steps of storing personal data in the form of a master user profile data structure which uniquely describes the user, together with a number of personal registration data structures, each of which describes registration data associated with the successful registration of the user with a service computer or server node.

10. A method according to claim 9, in which the personal registration data structures permit repeat visits to the service computer or server node without the user having to go through the registration procedure again.

11. A method according to claim 9 or 10, including the step of accepting user inputs which define a privacy policy in relation to the user's personal data which describes the extent to which the personal data is to be released for the purpose of submitting a registration application.

12. A method according to any of claims 9 to 11, including the step of providing a unique proxy address for the user in a registration application so that communications addressed to the user using the unique address are received by the at least one

registration agent computer or registration agent server and are subsequently forwarded to the user.

13. A method according to claim 12, in which the communications are forwarded to the user in dependence on an email filtering policy accepted by the user.

14. A method according to claim 13, in which a different proxy address for the user is allocated for each subsequent registration with other service computers or server nodes.

15. An apparatus for managing the registration of a user in accordance with the method of any preceding claim, comprising:

means for storing registration data;

means for storing personal data;

means for receiving a user request to submit a registration application on behalf of the user to a remote site;

means for completing a registration application based on a combination of personal data associated with the user and registration data associated with the remote site; and,

means for transmitting a completed registration application to the remote site on behalf of the user.

16. An apparatus according to claim 15, comprising a computer storage medium containing computer executable instructions for performing the method of any one of claims 1 to 14.

17. An apparatus according to claim 14, comprising a server.

18. An apparatus according to claim 17, in which the server is arranged to provide a website having a unique resource location (URL).

19. A memory for storing data comprising a data structure in said memory comprising a master user profile data structure which uniquely describes a user, together with a number of personal registration data structures, each of which describes registration data associated with the successful registration of the user with a service computer or server node.

20. A computer system for managing the registration of a user with a remote computer system comprising:

a memory storing registration data associated with one or more remote computer systems;

a memory storing personal data associated with one or more users;

a processor configured to accept a user request to submit a registration application on behalf of the user to a remote computer system, to complete a registration application based on a combination of personal data associated with the user and registration data associated with the remote computer system; and,

to submit the completed registration application to the remote site on behalf of the user.

21. A computer system hosting a WWW site adapted to facilitate registration of users by proxy comprising a memory holding the WWW site, the WWW site having embedded encoded information to allow the WWW site's registration data requirements to be determined automatically by a registration processing system.

22. A user interface and execution system for managing registration of a user with a service computer, wherein the user interface comprises:

memory means for storing registration data requirements for the at least one service computer in at least one data structure;

personal data input means for accepting personal data relating to the user;

memory means for storing at least part of the personal data in at least one data structure; and,

processing means being operative to accept a request to register the user with the at least one service computer, to compile a registration request from data obtained by accessing the user's personal data stored in the associated data structure and by accessing registration data for the service computer stored in the associated data structure and to register the user with the at least one service computer by transmitting the registration request to the service computer.

23. A method of registering with a number of service computer systems comprising the steps of

visiting a WWW site hosting a registration management system;

submitting a registration application to the registration management system comprising a user identifier, password and personal data; and,

instructing the registration management system to submit a registration to one or more of the service computer systems using the submitted personal data.

24. A method according to claim 23, further comprising the step of submitting inputs to the registration management system which define a privacy policy in relation to the user's personal data, the extent to which the personal data is released for the purpose of submitting a registration application being dependent on the privacy policy.

Fig.1.

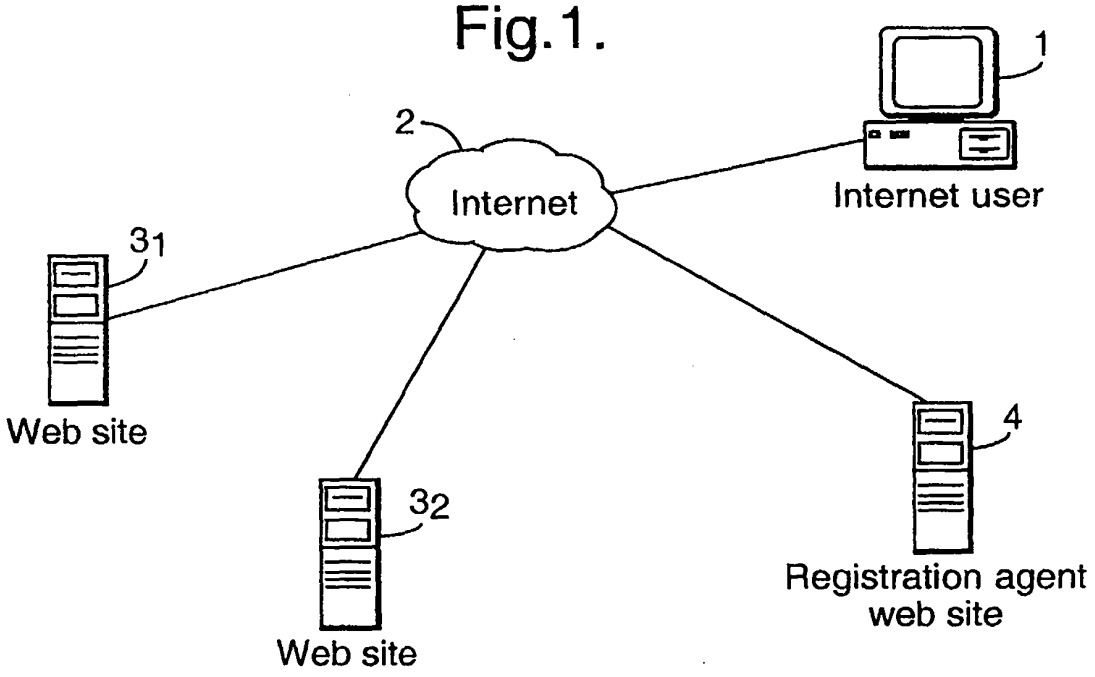

1
Internet user
2
Internet
31
Web site
32
Web site
4
Registration agent
web site

Fig.2.

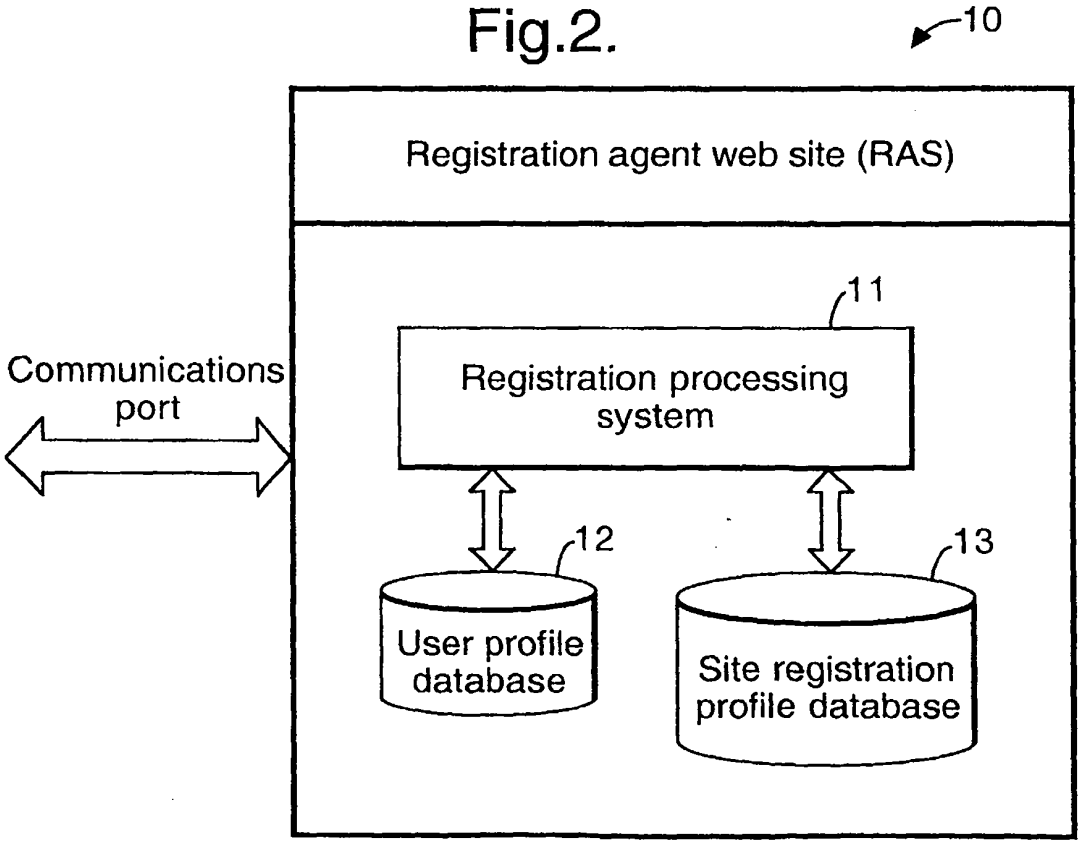

10
Registration agent web site (RAS)
11
Registration processing
system
Communications
port
12
User profile
database
13
Site registration
profile database

Fig.3.

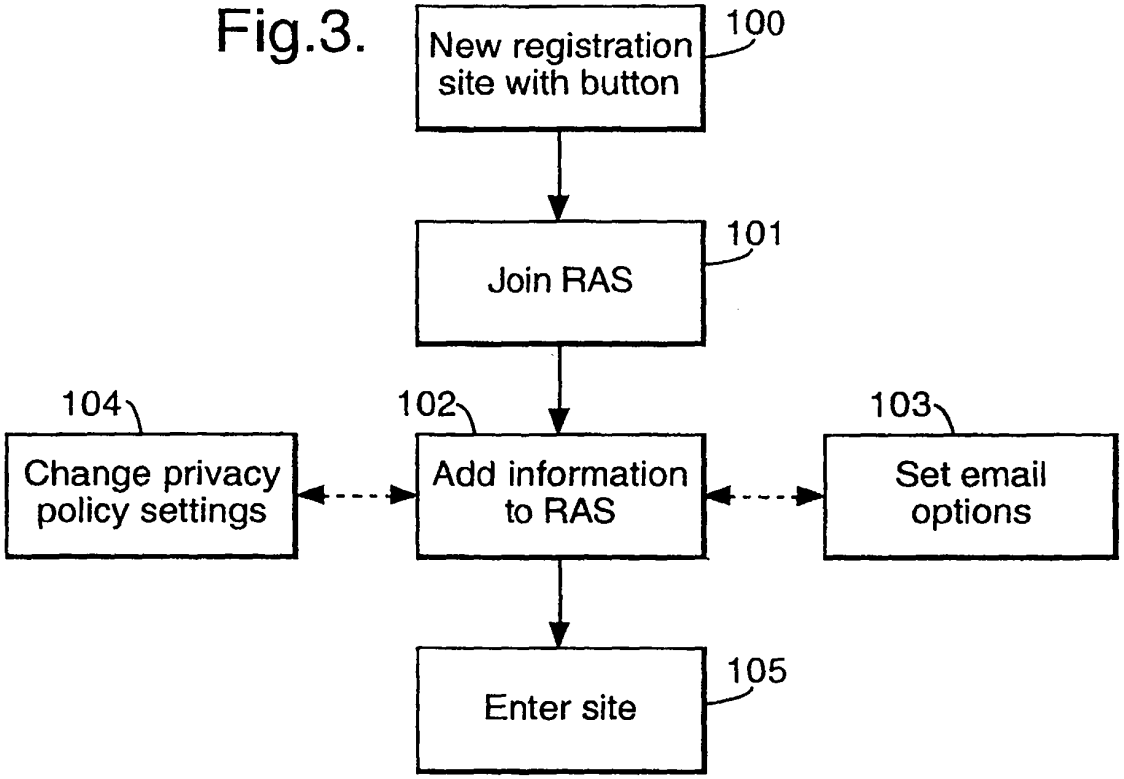

New registration site with button
100
Join RAS
101
104
102
103
Change privacy policy settings
Add information to RAS
Set email options
Enter site
105

Fig.5.

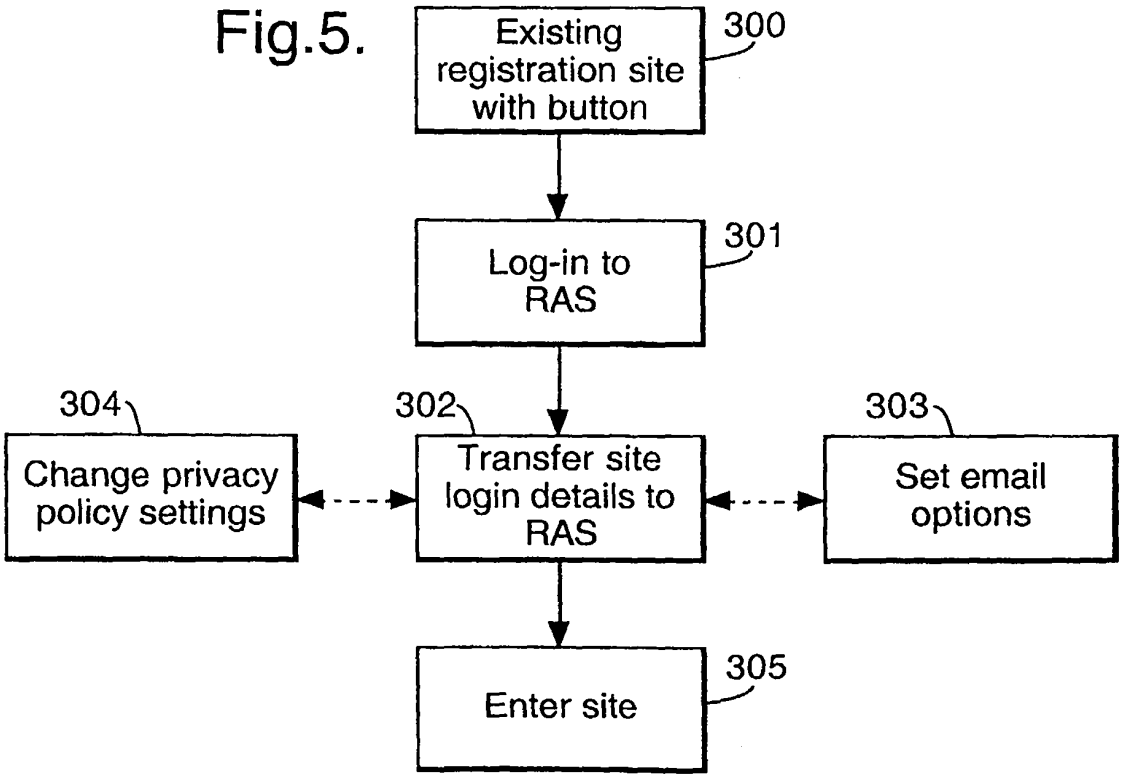

Existing registration site with button
300
Log-in to RAS
301
304
302
303
Change privacy policy settings
Transfer site login details to RAS
Set email options
Enter site
305

Fig.4.

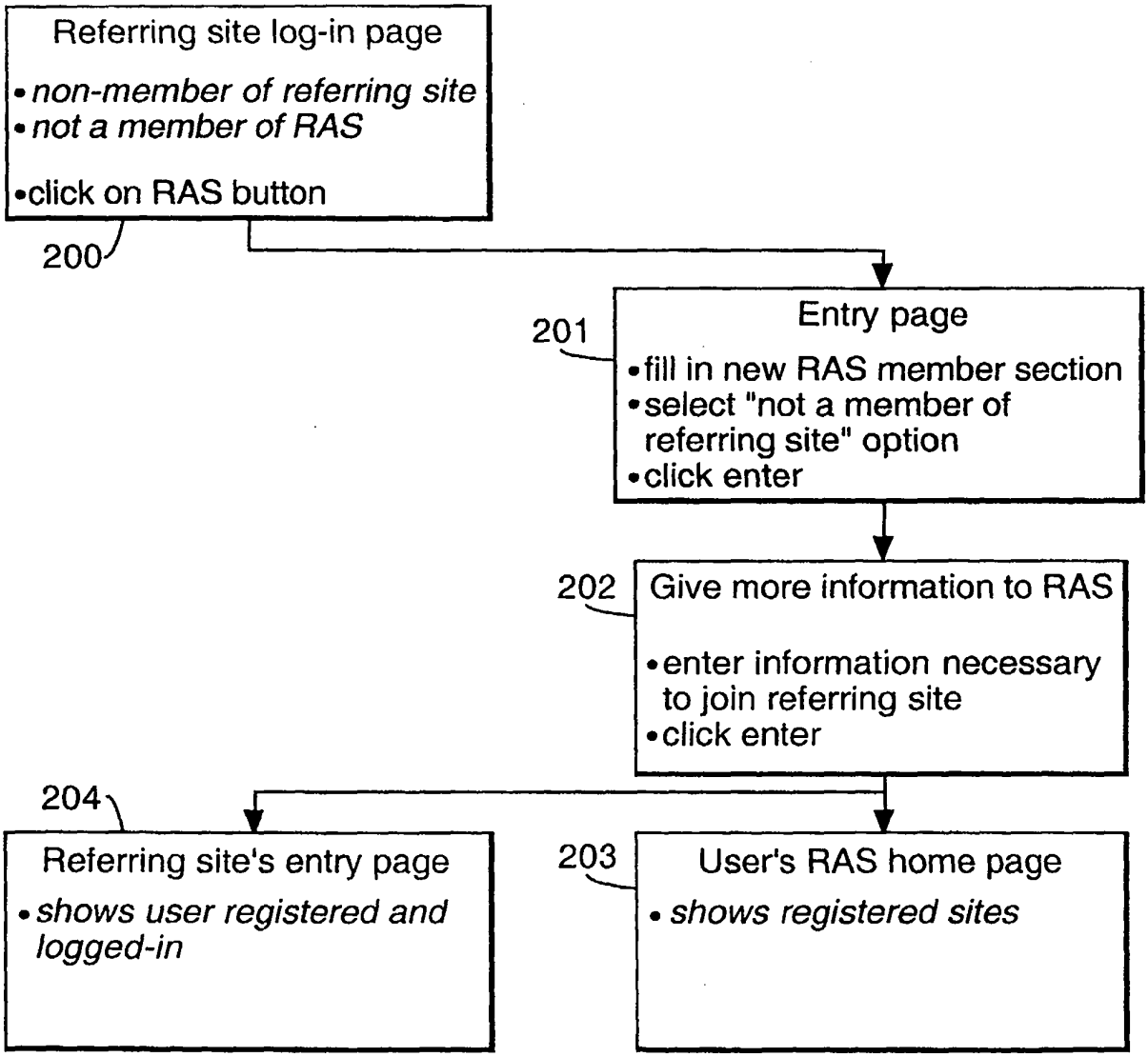
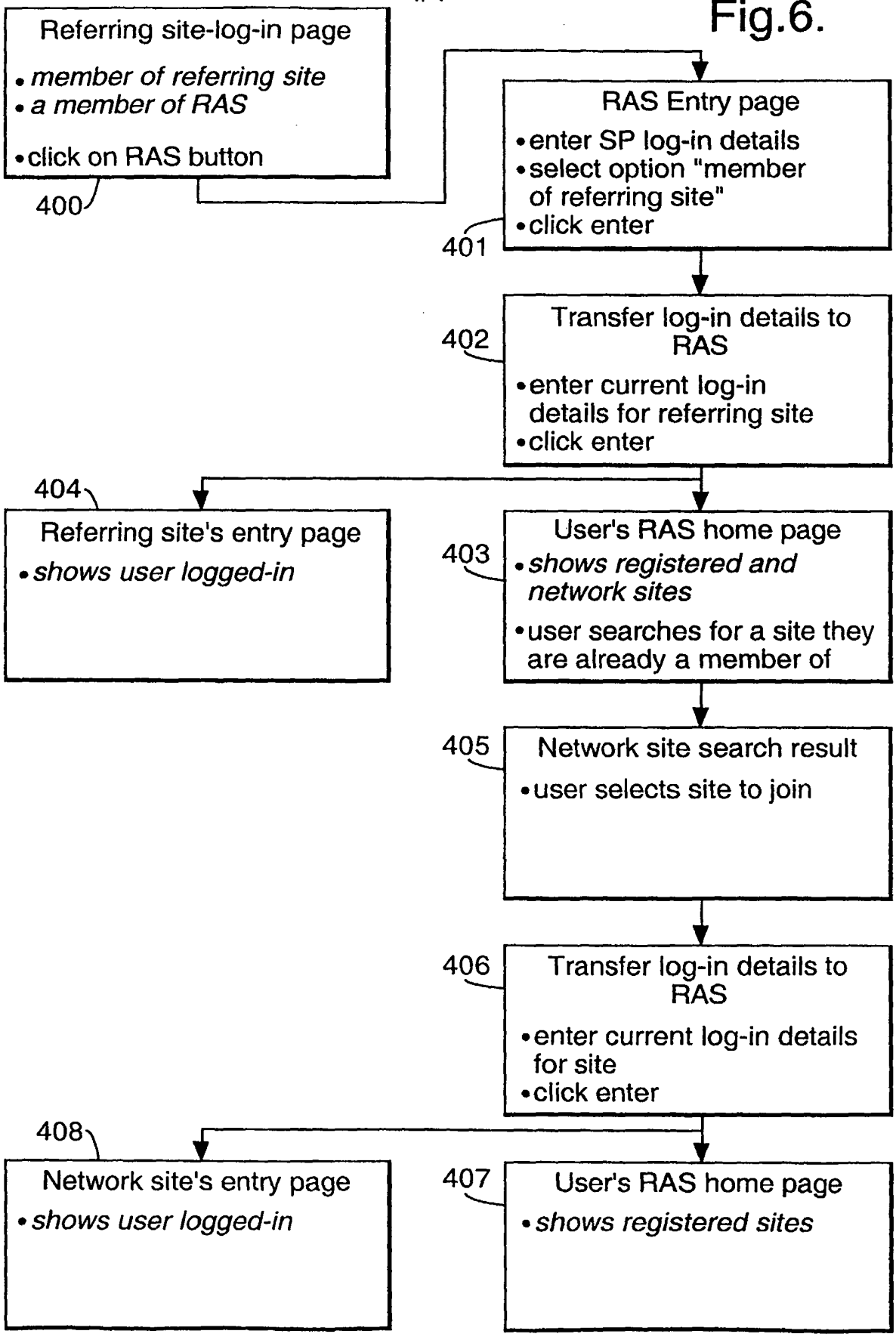

Referring site log-in page
• non-member of referring site
• not a member of RAS
•click on RAS button
200
201
Entry page
•fill in new RAS member section
•select "not a member of referring site" option
•click enter
202
Give more information to RAS
•enter information necessary to join referring site
•click enter
204
Referring site's entry page
• shows user registered and logged-in
203
User's RAS home page
• shows registered sites

Fig.6.


Referring site-log-in page
• member of referring site
• a member of RAS
• click on RAS button
400
RAS Entry page
• enter SP log-in details
• select option "member of referring site"
• click enter
401
Transfer log-in details to RAS
402
• enter current log-in details for referring site
• click enter
404
Referring site's entry page
• shows user logged-in
User's RAS home page
403
• shows registered and network sites
• user searches for a site they are already a member of
405
Network site search result
• user selects site to join
406
Transfer log-in details to RAS
• enter current log-in details for site
• click enter
408
Network site's entry page
• shows user logged-in
407
User's RAS home page
• shows registered sites

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/GB 00/00748

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 855 659 A (LUCENT TECHNOLOGIES INC) 29 July 1998 (1998-07-29)	19-24
A	column 3, line 16 -column 5, line 4 column 8, line 44 -column 9, line 7 column 14, line 56 -column 15, line 51 figures 3,4	1-18
A	US 5 764 890 A (MCKELVIE SAMUEL J ET AL) 9 June 1998 (1998-06-09) abstract column 1, line 39 -column 2, line 3 column 3, line 7-19 column 5, line 1-44	1-18

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 July 2000	21/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro Lõpez, M.L.

Form PCT/ISA/210 (second sheet) (July 1992)

Int. Jonal Application No
PCT/GB 00/00748

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 784 463 A (CHEN JAMES F ET AL) 21 July 1998 (1998-07-21) abstract column 2, line 27 -column 3, line 29 column 4, line 1-30 column 4, line 57-67 figures 1A,1B	1-18
A	US 5 544 322 A (CHENG PAU-CHEN ET AL) 6 August 1996 (1996-08-06) abstract column 3, line 12-35 column 5, line 43-63 column 6, line 38-58 column 8, line 37-63	1-18
T	BRIAN VAUGH & JAYNE MOONEY: "How to register a workstation" ZENWOKS COOL SOLUTIONS, 28 May 1999 (1999-05-28), XP002124920 Available from Internet<URL:http://www.novel.com/coolsolutions/zenworks/basics_ws_register.html> available on 28 May 1999 the whole document	1,2,5,8, 15-17
A	US 5 675 771 A (CURLEY JOHN L ET AL) 7 October 1997 (1997-10-07) column 4, line 16 -column 5, line 3 column 6, line 43-61 column 8, line 5-31	1-24
A	US 5 694 595 A (JACOBS DWAYNE CHARLES ET AL) 2 December 1997 (1997-12-02) column 2, line 1-25 column 4, line 28 -column 5, line 38	1-24

Patent document cited in search report	Publication dat	Patent family member(s)	Publication date
EP 0855659 A	29-07-1998	US 5961593 A	05-10-1999
		CA 2222480 A	22-07-1998
		JP 10254807 A	25-09-1998
US 5764890 A	09-06-1998	NONE	
US 5784463 A	21-07-1998	AU 5588198 A	29-06-1998
		WO 9825375 A	11-06-1998
US 5544322 A	06-08-1996	NONE	
US 5675771 A	07-10-1997	US 5983012 A	09-11-1999
		AU 679775 B	10-07-1997
		AU 7428994 A	13-04-1995
		CA 2132900 A	29-03-1995
		DE 69424842 D	13-07-2000
		EP 0646865 A	05-04-1995
		JP 7182180 A	21-07-1995
		US 5572711 A	05-11-1996
		US 5566326 A	15-10-1996
		US 5664098 A	02-09-1997
US 5694595 A	02-12-1997	NONE	

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07F 7/10, 19/00

A1

(11) International Publication Number: **WO 00/49586**

(43) International Publication Date: 24 August 2000 (24.08.00)

(21) International Application Number: PCT/IE00/00025

(22) International Filing Date: 18 February 2000 (18.02.00)

(30) Priority Data:

60/120,747	18 February 1999 (18.02.99)	US
60/129,033	13 April 1999 (13.04.99)	US
60/134,027	13 May 1999 (13.05.99)	US
60/144,875	20 July 1999 (20.07.99)	US
60/147,153	4 August 1999 (04.08.99)	US

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DE (Utility model), DK, DK (Utility model), DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

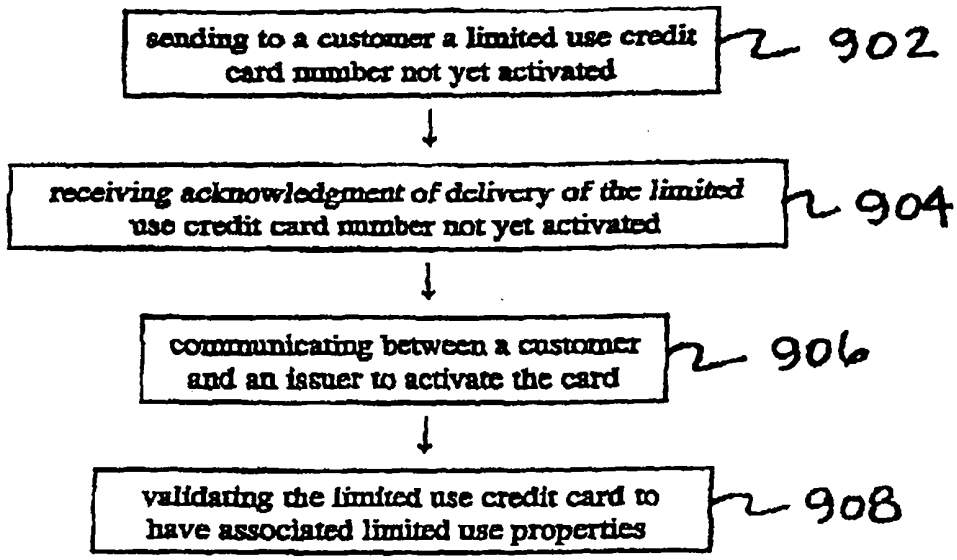
(71) Applicant *(for all designated States except US)*: ORBIS PATENTS LIMITED [IE/IE]; 181 Howth Road, Dublin 3 (IE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FLITCROFT, Daniel, Ian [GB/IE]; 70 Lower Albert Road, Sandycove, County Dublin (IE). O'DONNELL, Graham [IE/IE]; 5 Lower Albert Road, Sandycove, Dun Laoghaire, County Dublin (IE).

(74) Agents: O'CONNOR, Donal, H. et al.; Cruickshank & Co., 1 Holles Street, Dublin 2 (IE).

(54) Title: CREDIT CARD SYSTEM AND METHOD



(57) Abstract

A credit card system is provided which has the added feature of providing additional limited use credit card numbers and/or cards. These numbers and/or cards can be used for a single or limited use transaction, thereby reducing the potential for fraudulent reuse of these numbers and/or cards. The credit card system finds application to "card remote" transactions such as by phone or Internet. Additionally, when a single use or limited use credit card is used for "card present" transactions, so called "skimming" fraud is eliminated. Various other features enhance the credit card system which will allow secure trade without the use of elaborate encryption techniques. Methods for limiting, distributing and using a limited use card nubmer, controlling the validity of a limited use credit card number, conducting a limited used credit card number transaction and providing remote access devices for accessing a limited use credit card number are also provided.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

CREDIT CARD SYSTEM AND METHOD

Introduction

This invention relates to a credit card system and method, and more particularly, to a credit card system and method offering reduced potential of credit card number misuse.

The development of retail electronic commerce has been relatively slow in spite of the perceived demand for such trade. The single greatest deterrent to the expansion of retail electronic commerce is the potential for fraud. This potential for fraud has been a major concern for the credit card companies and financial institutions as well as the customers and the providers of the goods and services.

The former are concerned about fraud because essentially the financial institutions have to bear the initial cost of the fraud. Additionally, the credit card companies have an efficient credit card system which is working well for face to face transactions, i.e., "card present" transactions where the credit card is physically presented to a trader and the trader can obtain the credit card number, compare signatures and in many cases photographs before accepting a particular credit card.

The latter are equally concerned about fraud being well aware that ultimately the user must pay for the fraud. However, there are particular personal concerns for the consumer in that the fraudulent use of the credit card by misuse of the credit card number by a third party may not become apparent for some time. This can happen even if the card is still in his or her possession. Further, when fraud does occur the consumer has the task of persuading the credit card provider that fraud by another did indeed occur.

There is also the additional fear of being overcharged on a credit card. There are thus particular risks for those credit card holders who have relatively high spending limits, in that if fraud should occur, it may be some considerable time before it is detected. One

particular form of fraud referred to as "skimming" is particularly difficult to control. What happens is that the card holder proffers his or her card at an establishment to make a transaction, the relevant information is electronically and/or physically copied from the card and the card is subsequently reproduced. This can be a particular problem with travelers particularly during an extensive period of travel as the fraudulent card may turn up in other places and it may be some considerable time before the fraud is detected.

For remote credit card use, the credit card holder has to provide details of name, master credit card number, expiration date and address and often many other pieces of information for verification; the storing and updating of the information is expensive but necessary. This of itself is a considerable security risk as anybody will appreciate that this information could be used to fraudulently charge goods and services to the card holder's credit card account. Such fraudulent use is not limited to those people to whom the credit card information has been given legitimately, but extends to anybody who can illegitimately obtain such details. A major problem in relation to this form of fraud is that the credit card may still be in the possession of the legitimate holder as these fraudulent transactions are taking place. This is often referred to as "compromised numbers" fraud. Indeed all this fraud needs is one dishonest staff member, for example in a shop, hotel or restaurant, to record the credit card number. It is thus not the same as card theft.

The current approaches to the limiting of credit card fraud are dependent on the theft of a card being reported and elaborate verification systems whereby altered patterns of use initiate some inquiry from the credit card company. Many users of credit cards have no doubt received telephone calls, when their use of the card has been exceptional, or otherwise unusual in the eyes of the organization providing the verification services.

Thus, there have been many developments in an effort to overcome this fundamental problem of fraud, both in the general area of fraud for ordinary use of credit cards and for the particular problems associated with such remote use.

One of the developments is the provision of smart cards which are credit card devices containing embedded electronic circuitry that can either store information or perform computations. Generally speaking they contribute to credit card security systems by using some encryption system. A typical example of such a smart card is disclosed in U.S. Patent No. 5,317,636 (Vizcaino).

Another one of the developments is the Secure Electronic Transaction (SET) protocol which represents the collaboration between many leading computer companies and the credit card industry which is particularly related to electronic transmission of credit card details and in particular via the Internet. It provides a detailed protocol for encryption of credit card details and verification of participants in an electronic transaction.

Another method that is particularly directed to the Internet is described in U.S. Patent No. 5,715,314 (Payne et al.). U.S. Patent 5,715,314 discloses using an access message that comprises a product identifier and an access message authenticator based on a cryptographic key. A buyer computer sends a payment message that identifies a particular product to a payment computer. The payment computer is programmed to receive the payment message, to create the access message, and to send the access message to a merchant computer. Because the access message is tied to a particular product and a particular merchant computer, the access message can not be generated until the user sends the payment message to the payment computer. Because the access message is different from existing credit card formats, the access message is ill-suited for phone/mail orders and other traditional credit card transactions.

U.S. Patent No. 5,883,810 (Franklin et al.) describes an online transaction system in which a user of the Internet or the like clicks on an icon to receive a proxy transaction number from a credit card provider. This proxy number stands in for the user's regular credit card number during transmission over the Internet, but expires after a short time (e.g., one hour) to reduce the chance that the number will be effectively intercepted

and fraudulently used. The processing that occurs when a bank receives transaction information from a merchant involves checking whether the proxy number is a valid number and whether the transaction value and merchant match. There is no additional processing triggered when the bank processing system receives the proxy number. In addition, a significant drawback of the Franklin et al. system is that an unscrupulous merchant or a criminal who is capable of accessing or intercepting order details can then turn around and use the proxy number a number of times before the lapse of the expiration term. Thus, more than one transaction can occur within the duration of the expiration term. The Franklin et al. system has nothing in place to prevent this type of fraud. The Franklin et al. system merely depends upon an assumption that fewer criminals could obtain the proxy number and reuse it within the expiration term of the proxy transaction number set by the issuing bank than the total number of criminals capable of gaining access to credit card numbers used for online commerce. Also, the inclusion of specific transaction information does not prevent a fraudulent merchant from recurrent unauthorized charges within the expiry time of the proxy number. The user will not be aware of this misuse of his/her credit card details until the receipt of the statement, which will typically not be until several weeks later.

There are also specific electronic transaction systems such as "Cyber Cash," "Check Free" and "First Virtual." Unfortunately, there are perceived problems with what has been proposed to date. Firstly, any form of reliance on encryption is a challenge to those who will then try to break it. The manner in which access has been gained to extremely sensitive information in Government premises would make anyone wary of any reliance on an encryption system. Secondly, a further problem is that some of the most secure forms of encryption system are not widely available due to government and other security requirements. Limiting the electronic trading systems and security systems for use to the Internet is of relatively little use. In addition, entirely new electronic payment systems require changes in how merchants handle transactions and this represents an important commercial disadvantage for such systems.

Additionally, various approaches have been taken to make "card present" transactions more attractive. For instance, Japanese Patent Publication No. Hei 6-282556

discloses a one time credit card settlement system for use by, e.g., teenage children of credit card holders. This system employs a credit card which can be used only once in which various information such as specific personal information, use conditions, and an approved credit limit identical to those of the original credit card are recorded on a data recording element and displayed on the face of the card. The one-time credit card contains the same member number, expiration date, card company code, and the like as on existing credit card, as well as one-time credit card expiration date not exceeding the expiration date of credit card, available credit limit for the card, and the like. The one-time credit card makes use of some of the same settlement means as the conventional credit card. However, the system also requires use permission information to be recorded on the credit card, the information permitting the credit card to be used only once or making it impossible to use the credit card when the credit limit has been exceeded. A special card terminal device checks the information taken from the card for correctness and imparts use permission information for when the card is not permitted to be used on the transmission to the credit card issuing company. The use permission information takes the form of a punched hole on the card itself. This system has obvious drawbacks, such as the card terminal having to be modified for additional functions (e.g., punching holes, detected punched holes, imparting additional information, etc.). Also, such a system offers little additional security insofar as fraud can still be practiced perhaps by covering the holes or otherwise replacing the permission use information on the credit card. Further, such a system would require a change in nearly all card terminal equipment if it were adopted.

Patent Nos. 5,627,355 and 5,478,994 (Rahman et al.) disclose another type of system that uses a plurality of pin numbers which are added to a credit card number on an electronic display. U.S. Patent No. 5,627,355 discloses a credit card having a memory element containing a series of passwords in a predetermined sequence. These passwords are identical to another sequence stored in a memory of a host control computer. Further, the card contains a first fixed field containing an account number (e.g., "444 222 333"). In operation, the memory element of the credit card device provides a unique password from the sequence with each use of the credit

card-device. This permits verification by comparing the account number and the password provided with each use of the device with the account number and the next number in sequence as indicated by the host computer. The host computer deactivates the password after the transaction. Among the drawbacks with this type of system is the need for a power supply, a display, a memory device, a sound generator and the need to recycle a limited sequence of pin numbers. Such a system is not readily adapted to current credit card transactions because it lacks the ability of providing a check sum of the card number and cannot be read by a standard card reader. Also, if the card is lost or stolen, there is little to prevent a person from using the card until it is reported to be lost or stolen by the correct holder. See, also, U.S. Patent No. 5,606,614 (Brady et al.).

Other attempts have been made to make funds available to an individual, but with limitations. For example, U.S. Patent Nos. 5,350,906 (Brody et al.) and 5,326,960 (Tannenbaum et al.) disclose issuing temporary PINs for one time or limited time and limited credit access to an account at an ATM. These patents disclose a currency transfer system and method for an ATM network. In this system, a main account holder (i.e., the sponsor) sets up a subaccount that can be accessed by a non-subscriber by presenting a fixed limit card associated with the subaccount and by entering a password corresponding to the subaccount. Once the fixed limit is reached, the card can no longer be used. The fixed limit card contains information on its magnetic stripe pertaining to the sponsor account.

One of the problems with all these systems is that there are many competing technologies and therefore there is a multiplicity of incompatible formats which will be a deterrent to both traders and consumers. Similarly, many of these systems require modifications of the technology used at the point of sale, which will require considerable investment and further limit the uptake of the systems.

Summary of the Invention

Many solutions have been proposed to the problem of security of credit card transactions. However, none of them allow the use of existing credit cards and existing credit card formats and terminal equipment. Ideally, as realized by the present inventors, the solution would be to obtain the functionality of a credit card, while never in fact revealing the master credit card number. Unfortunately, the only way to ensure that master credit card numbers cannot be used fraudulently is to never transmit the master credit card number by any direct route, i.e., phone, mail, Internet or even to print out the master credit card number during the transaction, such as is commonly the case at present.

According to exemplary embodiments of the present invention as described in the present inventor's earlier application (U.S. non-provisional application 09/235,836), a more secure way of using existing credit cards and, in particular, using existing credit cards in remote credit card transactions was provided. The present invention is further directed towards providing a more secure way of using existing credit cards generally which will not require any major modifications to existing credit card systems. It is further directed towards providing a credit card system that will be user friendly and will provide customers with a greater confidence in the security of the system.

These and other advantages of the present invention are satisfied by a first exemplary embodiment, which pertains to a method used in a financial transaction system capable of using a limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of said at least one credit card number and which is associated the master account number of a customer. The method controls the validity of the limited use credit card number and includes the steps of: sending to a customer from a limited use credit card number issuer a limited use credit card number which is not yet activated; receiving acknowledgment of delivery by the customer of the limited use credit card number which is not yet activated; communicating with a limited use card number card issuer to activate the

card before it can be used in a transaction; and validating the limited use credit card to have associated limited use properties. These properties can be such things as a specific time period, a specific merchant, a specific group of merchants, a specific type of transaction, and a specific number of transactions.

The validation step can include activating validity limited credit card software using a user identification to identify the user with the card issuer; requesting validation of a limited use credit card for a merchant as identified by a merchant identification number; and providing an option for a user to specify additional limitations other than the specific merchant to the limitation on the limited use credit card number.

Additionally, the present invention provides a method of conducting a limited use credit card transaction, which includes initiating a transaction by a customer presenting a limited use credit card number to a merchant; routing said limited use credit card number to a central processing system; determining whether said limited use credit card number has been deactivated because the limited use condition has been satisfied; transmitting a signal to the merchant denying authorization of the card number if the credit card number has been deactivated; transmitting a signal to a master credit card issuing facility which issued that limited use credit card number, said signal including original transaction details but with the limited use credit card number remapped to be a master credit card number if said limited use credit card number has not been deactivated; determining at the whether authorization can be obtained against the master credit card number; authorizing or denying authorization of the transaction based on this determination; remapped any such authorization or denial to the limited use credit card number for transmission to the merchant; and transmitting a signal to the merchant authorizing or denying authorization of the limited use credit card number.

Further, the present invention provides a method of conducting a settlement transaction including transmitting a signal from a merchant to a central processing system according to a BIN of the limited use card number; remapping the limited use credit card number with the master credit card number; transmitting said remapped

master credit card number to issuer processing facility which issued the master credit card number; settling the transaction by payment, if appropriate, to the central processing system; remapping the master credit card number back to the limited use credit card number; and transmitting the limited use credit card number and payment information, if appropriate, to the merchant.

Furthermore, the present invention includes a method of providing remote access devices for accessing limited use numbers. The method includes submitting user authentication information and the master account number for entry into a database; determining whether the user is a valid user of the master credit card number; registering the user if the user is determined to be a valid user; obtaining by registered users a software package to which enables communication with a remote access device support server to enable the issuance of limited use card numbers; using the software package to initiates communication with the remote access support server; authenticating the user at the remote access support server; requesting a limited use number by an authenticated user; specifying by the authenticated user any additional transaction limitations desired; obtaining an available limited use number; entering the limited use number and the specified limitations into the database such that the limited use number is associated with the user's information already in database; and transmitting the limited use number to the user.

In this way, a merchant can receive a limited use credit card number; process the received limited use credit card number in a transaction as any other credit card number; pass the transaction through to the card issuer's processing system; and request authorization of the transaction at the card issuer's processing system against the associated limited use properties. The system can then deactivate the limited use credit card number by the card issuer when a use-triggered condition is present. Also, limited use transaction numbers can be obtained by authorized users and transactions can be processed within the existing credit card system with only minor modifications.

DETAILED DESCRIPTION OF THE INVENTION

The present invention will be more readily understood upon reading the following detailed description in conjunction with the drawings in which:

Fig. 1 shows an exemplary system for implementing the present invention;

Fig. 2 shows, in high-level form, the operation of the central processing station shown in Fig. 1;

Fig. 3 is a flow chart illustrating an exemplary process for allocating credit card numbers;

Fig. 4 is a flow chart illustrating an exemplary process for limiting the use of a credit card number;

Fig. 5 is a flow chart illustrating an exemplary process for distributing credit card numbers;

Fig. 6 is a flow chart illustrating an exemplary process for electronically using credit card numbers;

Fig. 7 is a flow chart illustrating an exemplary process for processing a transaction;

Fig. 8 is a flow chart illustrating another exemplary process for processing a transaction;

Fig. 9 is a flow chart illustrating an exemplary method of controlling the validity of a limited use credit card number;

Fig. 10 is a flow chart illustrating an exemplary process for using a credit card

— number as a PIN number;

Fig. 11 is a block diagram illustrating an exemplary location for the central processing system;

Fig. 12 is a flow chart illustrating an exemplary method of conducting a limited use credit card number transaction;

Fig. 13 is a flow chart illustrating an exemplary method of conducting a settlement transaction;

Fig. 14 is a block diagram illustrating an alternate exemplary location for the central processing system;

Fig. 15 is a block diagram illustrating an alternate exemplary process for limiting, distributing and using a limited use card number; and

Fig. 16 is a flow chart illustrating an exemplary method of providing remote access devices for accessing limited use credit card numbers.

In this specification the term "credit card" refers to credit cards (MasterCard®, Visa®, Diners Club®, etc.) as well as charge cards (e.g., American Express®, some department store cards), debit cards such as usable at ATMs and many other locations or that are associated with a particular account, and hybrids thereof (e.g., extended payment American Express®, bank debit cards with the Visa® logo, etc.). Also, the terms "master credit card number" and "master credit card" refer to the credit card number and the credit card as generally understood, namely, that which is allocated by the credit card provider to the customer for his or her account. It will be appreciated that an account may have many master credit cards in the sense of this specification. For example, a corporation may provide many of its employees with credit cards but essentially each of these employees holds a master credit card even if there is only one customer account. Each of these master credit cards will have a

unique master credit card number, which set of master credit card numbers will be linked to the account. Similarly, in families, various members of the family may hold a master credit card, all of which are paid for out of the one customer account.

Additionally, the "master credit card" account can be in some embodiments something other than a credit card account. For instance, while not otherwise affecting the formatting or processing of the limited use credit card numbers as described herein, the master card number can be a prepaid account or another type of account, such as a utility, telephone service provider or Internet Service Provider (ISP) account. The utility company, telephone company, ISP or other account holder would generate a bill, which, in possible addition to or separate from to the regular bill, would include a listing of limited use credit card transactions. An advantage of this type of arrangement is that the service provider already has information as to a pool of individual and their credit worthiness, as well as low increased overhead due to the already in place billing system. In these embodiments, the "master account" may but likely does not have the format of a standard credit card or the like.

The term "limited-use" credit card number is used to encompass at least both the embodiment in which the credit card is designated for a single use, and the embodiment in which the credit card is designated for multiple uses providing that the charges accrued do not exceed a prescribed threshold or thresholds, such a total single charge, total charges over a limited time period, total charge in a single transaction, etc. A common feature is that the limitation is based on a use-triggered condition subsequent, and not just the expiration date of the card. Stated differently, the a limited-use credit card number is deactivated upon a use-triggered condition which occurs subsequent to assignment of said at least one credit card number.

The terms "card holder" and "user" are used interchangeably to refer to an entity, e.g., an individual, that has been rightfully issued a credit/debit/charge card number, e.g., through a contractual arrangement, or that has been authorized to use such card by such entity or a representative of such entity.

There are at least two basic different ways of carrying out the present invention. In summary, they are the allocation of additional credit card numbers for remote trade and secondly the provision of what are effectively disposable credit cards for remote and card present trade, both of which have the feature of in the case of single use or in the case of multiple use, protecting against the worst effects of compromised numbers fraud or skimming.

In a refinement of the invention, it is possible to control the manner in which an actual transaction is carried out as a further protection against unscrupulous providers of goods and services.

Essentially, there are certain matters that will be considered in relation to this invention. They are firstly the operational or functional features in so far as they affect customers, and then there are the technical features, namely how the invention is implemented, how the invention is provided to the customers, and finally, how the invention is handled by the providers of goods and services and the processors of the credit cards, i.e., the financial institutions and/or their service providers.
The operational or functional features of this invention will be discussed first in the context of a standard credit card system.

One basic feature of the invention is to provide in a credit card system such that each master credit card holder could be provided with one or more of the following: 1) additional single use credit card numbers for remote transactions; 2) multiple use credit card numbers for remote transactions; 3) single use additional credit cards for remote and card present transactions; and 4) multiple use credit cards for remote and card present transactions.

It is also envisaged that in certain situations credit cards can be provided to people who do not have an account with any credit card company. This latter feature is described in more detail below. Various other features may be provided in the above situations, which will further improve the security of credit card transactions.

Dealing firstly with the situation where a master credit card holder has an additional credit card number allocated to him or her for a single use, it will be appreciated that since the number can only be used for one single transaction, the fact that the number is in anybody else's hands is irrelevant as it has been deactivated and the master credit card number is not revealed to the third party. Various other features may be added to such single use credit card numbers, for example, the value of the transaction can be limited, thus the master credit card holder can have a plurality of single use credit card numbers of differing values. For example, when a remote trade is carried out, the master credit card holder will use a credit card number which has a credit card limit only marginally above or equal to that of the value of the transaction. This would reduce the chances of or prevent an unscrupulous trader using the credit card number to supply additional goods or services over those ordered or to increase the agreed charge.

A second embodiment of the invention provides the master credit card holder with an additional credit card number for use in remote trade, which credit card number could have, as in the previous example of the invention, a credit limit for each specific transaction or a credit limit such that when the aggregate amount of a series of transactions exceeded a specific credit limit that the credit card number would be canceled, invalidated or in some other way deactivated. Similarly, the multiple use credit card number could be limited to, for example, five uses with a credit limit not exceeding $100 in each transaction and an aggregate credit limit not exceeding $400. Similarly, a time restriction could be put on such a credit card number in that it would be deactivated if it was used with frequency above (or below) a given threshold, for example, more than once a week. It will be appreciated that the limits that can be placed on the use of a single use credit number or a multiple use credit card number are almost limitless and those having skill in the art will consider other ways in which the use of the credit card number could be limited, whether it be by time, by amount, frequency of use, by geographical region, by merchant, by merchant class, or by purpose or use (such as limited to Internet trade and so on), or by some combination of these separate criterion.

The third way in which the invention could be carried out is by physically providing additional single use credit cards each of which would have a unique additional credit card number. Such additional single use credit cards could then be used both for remote trade by using the additional credit card numbers for respective transactions, and for "card present" trade where each card would be "swiped" in the normal manner. Such a disposable credit card could be made like any common credit card, or from a relatively inexpensive material, such as cardboard or thin plastic, with the relevant information entered into it in readable (e.g., magnetic) form, as is already the case with many forms of passes for use in public transport and the like. Again, substantially the same features as with the credit card number could be provided. Thus, for example, the disposable credit card could be limited to use geographically, to a use, to an amount, to a frequency of use, to an expiration date, and so on. Again, those skilled in the art will appreciate that there are many variations to this concept.

Another way of carrying out the invention is to provide a master credit card holder with a multiple use additional credit card, where the additional credit card provides any limitations as to use triggered conditions subsequent that may be desired.

Ideally, irrespective of the manner in which the invention is carried out, the master credit card holder would be provided with either a plurality of single use additional credit card numbers or multiple use credit card numbers or a mixture of single and multiple use credits cards.

It will be appreciated that with either single use credit card numbers or single use additional credit cards, it is possible to eliminate or reduce the risk of credit card number fraud. Further, depending on the credit limit imparted to the particular credit card number or additional credit card number or single use additional credit card, it is possible to further limit the possibilities of fraud in any remote transaction and that with the use of a disposable single use credit card it is possible to eliminate or reduce the risk of skimming.

With multiple use additional credit card numbers and multiple use additional credit cards, the above-identified problems may not be totally eliminated due to preferences of the user. This is because, in certain circumstances, credit card users may prefer to have, for example, an additional credit card number for remote trade with a specific credit limit that they use all the time and are willing to take the risk of compromised number fraud, in the sense that they can control the severity of this misuse. This would be particularly the case where some of the various user triggered conditions subsequent limitations suggested above are used with the additional credit card number. Substantially the same criteria would apply to an additional multiple use credit card.

Effectively, the present invention solves the problem by obtaining the functionality of a credit card while never in fact revealing the master credit card number as the master credit card number need never be given in a remote transaction. Further, the master credit card itself need never be given to a trader.

In another embodiment of the invention, it is envisaged that people who do not hold master credit cards could purchase disposable credit cards which would have a credit limit for the total purchases thereon equal to the amount for which the credit card was purchased. These could then be used for both card present and card remote trade, the only proviso being that if the credit limit was not reached it will then be necessary for a refund to be given by the financial institution or credit card provider. An obvious way of obtaining such a refund would be through an automatic teller machine (ATM). In this way, the existing credit card transaction system is employed and the card holder is given the convenience of having a credit card.

As an alternative, the above-discussed cards could be, in effect, debit cards in the true sense, in which funds are withdrawn against a customer's account. In this case, the "credit card" issued, whether it be a one time use card or multi-use card, and whether have a credit limit or not, would be used to debit the account immediately. Preferably, the credit card issued in these circumstances would be single use with or without a transaction amount limit which would be used and processed by the

customer and merchant for a transaction as if it were a credit card, while in the customer's bank it would be treated like any other debit to the account.

Various aspects of the invention may be embodied in a general purpose digital computer that is running a program or program segments originating from a computer readable or usable medium, such medium including but not limited to magnetic storage media (e.g., ROMs, floppy disks, hard disks, etc.), optically readable media (e.g., CD-ROMs, DVDs, etc.) and carrier waves (e.g., transmissions over the Internet). A functional program, code and code segments, used to implement the present invention can be derived by a skilled computer programmer from the description of the invention contained herein.

Fig. 1 shows an exemplary overview of a system for implementing the limited use credit card system of the present invention. The system 100 comprises a central processing station 102, which, accordingly to exemplary embodiments, may be operated by the credit card provider. Generally, this station 102 receives and processes remotely generated credit card transactions. The credit card transactions can originate from a merchant in the conventional manner, e.g., by swiping a credit card through a card swipe unit 106. Alternatively, the credit card transaction requests can originate from any remote electronic (e.g., a personal computer) device 104. These remote devices can interface with the central processing station 102 through any type of network, including any type of public or propriety networks, or some combination thereof. For instance, the personal computer 104 interfaces with the central processing station 102 via the Internet 112. Actually, there may be one or more merchant computer devices (not shown) which receive credit card transactions from the remote electronic device 104, and then forward these requests to the central processing station 102. The central processing station 102 can also interface with other types of remote devices, such as a wireless (e.g., cellular telephone) device 140, via radiocommunication using transmitting/receiving antenna 138.

The central processing station 102 itself may include a central processing unit 120, which interfaces with the remote units via network I/O unit 118. The central

processing unit 120 has access to a database of credit card numbers 124, a subset 126 of which are designated as being available for limited use (referred to as the "available range"). Also, the central processing unit 120 has access to a central database 122, referred to as a "conditions" database. This database is a general purpose database which stores information regarding customers' accounts, such as information regarding various conditions which apply to each customers' account. Further, this database 122 may store the mapping between a customer's fixed master credit card number and any outstanding associated limited use credit cards, using, for instance, some type of linked-list mechanism. Databases 122 and 124 are shown separately only to illustrate the type of information which may be maintained by the central processing station 102; the information in these databases can be commingled in a common database in a manner well understood by those having skill in the data processing arts. For instance, each limited use credit card number can be stored with a field, which identifies its master account, and various conditions regarding its use.

The central processing unit 120 can internally perform the approval and denial of credit card transaction requests by making reference to credit history information and other information in the conventional manner. Alternatively, this function can be delegated to a separate clearance processing facility (not shown).

Finally, the central processing station includes the capability of transmitting the limited use credit card numbers to customers. In a first embodiment, a local card dispenser 128 can be employed to generate a plurality of limited use cards 132 and/or a master credit card 134 for delivery to a customer. In a second embodiment, the limited use credit card numbers can be printed on a form 136 by printer 130, which is then delivered to the customer via the mail. The printed form 136 may include material which covers the numbers until scratched off, thereby indicating what numbers have been used and are no longer active. This listing of numbers can be included in a monthly or other periodic account statement sent to the customer. In a third embodiment, these limited use numbers can be electronically downloaded to a user's personal computer 104, where they are stored in local memory 142 of the personal computer 104 for subsequent use. In this case, the credit card numbers can be

encrypted (described in detail later). Instead of the personal computer 104, the numbers can be downloaded to a user's smart card though an appropriate interface. In a fourth embodiment, the single-use credit card numbers can be downloaded to a radio unit 140 (such as a portable telephone) via wireless communication. In a fifth embodiment, an ATM 108 can be used to dispense the limited use cards 110. Those skilled in the art will readily appreciate that other means for conveying the numbers/cards can be employed. These embodiments are, of course, usable together.

The logic used to perform the actual allocation and deactivation of limited use credit card numbers preferably comprises a microprocessor, which implements a stored program within the central processing unit 120. Any general or special purpose computer will suffice. In alternative embodiments, the logic used to perform the allocation and deactivation of the limited use credit card numbers may comprise discrete logic components, or some combination of discrete logic components and computer-implemented control.

Fig. 2 shows a high-level depiction of the functions performed by the central processing station 102 or the like. The process begins in step 202 by allocating one or more limited use numbers to a customer. These numbers are ultimately selected from the list 126 of available limited use numbers, or some other sub-set list which has been previously formed from the numbers in list 126. Also, although not shown in Fig. 2, a master account number would have been preferably assigned to the customer at a previous point in time. The conditions database 122 may comprise a mechanism for associating the master account number (which can be a credit card number or some other type of account) number with the limited use credit card number. Because the limited use cards are arbitrarily chosen from the listing 126 of limited use card numbers, there should be no discernable link which would allow anyone to determine the master credit card number from any of the limited use numbers.

The processing then advances to step 204, where it is determined whether a customer requests or an event triggers a request for additional limited use cards or

card numbers. If so, additional limited use cards or card numbers are allocated to the customer.

Processing then advances to step 206, where the central processing station determines whether a transaction has taken place using a previously issued limited use card. This step is followed by a determination (in step 208) whether the limited use number should be deactivated. For instance, if the card is a single-use card, it will be deactivated. If the card is a fixed-limit card, the card is only deactivated if the recent transaction exceeds some stored threshold limit. These threshold limits can be stored on the card itself or in the conditions database 122. The actual step of deactivating is performed by generating a deactivation command, as represented in step 210 shown in Fig. 2. Naturally, there are other steps to processing a credit card transaction, such as checking whether the card is deactivated or otherwise invalid prior to completing the transaction. These additional steps are system specific and are not discussed here for sake of brevity.

Once a number is deactivated, this number can not be fraudulently reused. Hence, the risk of fraudulent capture of these numbers over the Internet (or via other transmission means) effectively disappears. In an alternative embodiment of the invention, these deactivated numbers can be reactivated providing that a sufficiently long time since their first activation has transpired. Providing that there is a sufficiently large number of limited use credit card numbers to choose from, it would be possible to wait a long time before it was necessary to repeat any numbers. At this point, it would be very unlikely that someone who had wrongfully intercepted a credit card number years ago would be motivated to fraudulently use it before the rightful owner.

After the limited use card is deactivated or a number of limited use cards are deactivated, an additional limited use card or cards can be activated. As described in detail in the following section, the actual activation of the credit card number can involve various intermediate processing steps. For instance, the credit card numbers from the list 126 can be first allocated to an "allocated" range of numbers, and then to an "issued but not valid" range of numbers, and then finally to an "issued and valid"

range of numbers. Fig. 2 is a high-level depiction of the process, and encompasses this specific embodiment, as well as the more basic case where the credit card numbers are retrieved from a database and then immediately activated.

Having set forth a summary of how the invention can be implemented, further details are provided in the following.

The first thing that the credit card provider should do is to generate a list of additional credit card numbers, whether they be single use or multiple use, and allocate additional credit numbers to a master credit card as a further credit card number for optional use instead of the master credit card number. Such a list can be produced by any suitable software package in the exemplary manner discussed in more detail below. Since the numbers allocated to a particular master credit card holder will not have any link to the master credit card number, the master credit card number should not be able to be derived from the additional credit card numbers.

In effect, randomness in credit card numbers is provided by the fact that there is a queue formed by the customers requiring numbers. Further, it should not be possible, even knowing the additional credit card numbers in a particular master credit card holder's possession which he or she may have used, to predict the next set of numbers that that particular master credit card holder will be allocated, since there will be randomness of access to additional credit card numbers in the truest sense. Even if the credit card provider were to allocate numbers sequentially, there would be no way of predicting the number that that credit card holder would subsequently acquire, since the numbers would be allocated by virtue of a queue, the randomness of this allocation being such as to prevent any prediction.

As such, the credit card numbers generated by the central computer need not be *per se* random numbers. Preferably, though, these numbers are valid credit card numbers with the constraint that they must conform to industry specifications of the format in terms of their numerical content in such a way that they can be handled with no (or minimal) modifications by merchant/acquiring systems and networks and be routed to

the appropriate center for processing. An additional constraint is that they must be different from all other conventional account numbers and all other single use numbers during their lifetime of validity. These constraints are practical requirements to produce a commercially viable system, which would likely not be satisfied by any process that generates random numbers in isolation.

To achieve these allocation requirements, an issuing bank decides within its total available range of credit cards to allocate a certain range or ranges of numbers to the single use system, referred to herein as the "available range." This may represent spare numbers using existing header sequences (e.g., the sequence of usually 4-6 digits that define the issuing institution and are used to route the card to the appropriate transaction processor) or within newly created header sequences. The numbers not allocated include existing credit card accounts for that issuer and sufficient spare capacity for new account holders and replacement numbers for existing customers. The additional non-embossed components of the card details and any card specific information that is transmitted during a transaction may be varied from card to card to enhance security and privacy of credit card transactions.

Although each limited use number is unique during the its lifetime of validity, information required to route the card number and transaction details to the appropriate processor is maintained to ensure that limited use numbers are processed appropriately. However, the limited use numbers do not need to include either the master card account number or an encoded version of the account number. Indeed privacy and security are enhanced when no unique account holder identifier is included within the limited use credit card number.

Also, information that is verified prior to the card being processed for authorization and payment, such as expiry date and checksum digit must be valid. This information may vary from limited use number to limited use number, but must be valid to ensure that the number passes checks that may be completed within the merchant terminal, i.e., the checksum is appropriately calculated for each limited use number and the associated expiry date is valid at the time of use.

Within the constraint of using a valid credit card format, the random allocation process used to generate lists of unique limited use numbers can involve allocation from a range of numbers in which either the entire number or portions of the account number are varied. In addition, the allocation can include combinations of all or part of the account number together with all or part of additional information such as non-embossed additional numbers, expiry date and other information that identifies the card and is passed on by the merchant to the card processor during a transaction.

Sequential random allocation from a list of available valid credit/debit/charge card codes that have been solely allocated for use as limited use numbers ensures that the criteria specified for limited use numbers are met, i.e., no two limited use numbers are the same, no limited use number is the same as an existing account number, and no newly issued conventional card number is the same as a previously issued limited use number. To achieve true computational independence between account numbers and limited use cards and between limited use numbers for the same account, the random allocation process requires a truly random seed value. Such true randomness can be obtained from a physically random system with well defined properties such as a white noise generator. An analog to digital converter that receives an analog signal from such a truly random physical system can be used to ensure truly random allocation.

Other approaches can result in the same result with lower computational efficiency. For example the allocation process could randomly select valid credit card numbers within the entire range for a given card issuer and then discard the number if it is already in use as a limited use or conventional card number or if the same number was allocated within a given time frame.

The above process generates a series of available single use numbers. To repeat, the allocation process is achieved by a truly random (or less ideally a pseudo random) mapping process in which a single use number is randomly selected and then assigned to a selected account holder (either an existing credit/debit card holder, a new solely single use account holder or a bank account). Additional single use

numbers can be allocated for purchase on an individual basis. Each assigned single use number is then removed from the sequence of available numbers before the next allocation, ensuring a unique allocation of each single use number. An alternative mechanism for performing direct allocation to a specific account holder is for lists of single use numbers to be allocated to unique storage locations. The list from a specific storage location can then be directly allocated to a given account at a later date. This allows for rapid allocation of cards to new customers without any delay arising from the need to perform a new allocation procedure for each new customer.

This allocation process generates another series of single use numbers, the "allocated range" with an associated identification field to determine how the account will be settled once used, i.e., onto whose account the transaction will be charged. The allocation process can occur a significant time before the single use numbers are required. Once allocated, they are not added into the list of valid accounts until required by the user.

Fig. 3 is a flow chart illustrating an exemplary process for allocating credit card numbers. A central processing unit (CPU) generates a database of credit card numbers (step 302), and may select a master credit card number. (Step 304). In step 306, the CPU checks to make sure that the master credit card number is not the same as another credit card number. The CPU selects additional credit card numbers to allocate to the master credit card number or other type of account number. (Step 308). The CPU can use any of the techniques discussed above to select the additional numbers. In step 310, the CPU checks to make sure that the additional numbers are not the same as another credit card number. The additional numbers can be used, for example, for single use cards.

When a customer needs single use cards, the CPU can issue the additional credit card numbers to the customer. Unless these single use numbers are issued directly into the hands of the customer (e.g., by an automated teller machine (ATM)), they are not directly added to the list of valid account numbers held within the central computer system. These numbers are added to an "issued, but not valid" list of numbers. (Step

312). The number of single use numbers issued at one time depends upon the rate at which the customer will use the cards and the capability of the device used to store the single use numbers until used. The CPU can provide the customer with enough single use numbers to fulfill their single use purchase requirements for up to, for example, 2 years. Each single use number can be endowed with specific restrictions in terms of transaction type or value, provided that these properties do not exceed the restrictions placed up on the customer's account (such as the available credit balance).

Once a series of single use numbers are issued, the user has the option of confirming receipt by telephone before any of the issued numbers become validated on the processing system. (Step 314). Once receipt has been confirmed (or assumed), not every issued single use number is added to the "issued and valid" list. (Step 316). To prevent excessive valid single use numbers being held within the processing system, the number of single use numbers declared to be valid at any one time is limited to account for waste of numbers (i.e., numbers that are accessed by a customer but are never used to complete a transaction) and to allow for time delays between different transactions leading to differences in the sequence in which single use numbers are accessed by the customer and the sequence in which they arrive at the processing center. The maximum number of single use numbers valid at any one time can be determined by the card issuer but would be preferably in the range of 5-10. In the case of any attempted use outside the allocated range, the next single use number can be used as an additional identifier to validate the transaction. In this case, only a subset of the digits should be given by the user to prevent a fraudulent trader being able to gain access to multiple unused single use numbers. As soon as a single use number is invalidated (step 320) on use (step 318), an additional number from the "issued not valid" list for that customer is allocated to the "issued and valid" list, ensuring a continual supply of single use numbers up to the maximum allowed until the next set of single use numbers are issued. (Step 322).

In relation to the actual supply of the additional credit card numbers, this will not cause any difficulties to the credit card provider. For example, with a standard master credit

card number, there are up to fifteen or more digits, the first of which is used to identify the credit card provider, e.g., American Express®, VISA®, Mastercard®, etc. For major banks, three digits are used to identify the issuing bank. The last digit in a typical sixteen digit master credit card number is a checksum used to confirm that the number is a valid number. This leaves a total of up to 11 digits or more for the account identifying number and the expiration date. In some instances, the expiration date may not be sent back for clearance, while with certain credit card providers, additional credit card numbers or even additional information is required for clearance. For example, certain credit card providers print additional numbers on the card, which additional numbers are not embossed on the card and do not form part of the master credit card number. These additional printed and non-embossed credit card numbers can be used to identify that the person proffering the card for a non-card present transaction is actually in possession of the card when the order is made whether it be in writing or by phone. There are many devices, digits, pieces of information, etc. used by a credit card issuer or processor working for a credit card issuer to clear the credit card for the specific transaction. According to another embodiment, when issuing additional credit card numbers in accordance with the present invention, such additional credit card numbers could include a code which would identify that the person using the additional credit card number in a remote transaction is the one to whom the numbers were sent or, in the case of a disposable credit card, is the one to whom the disposable credit card was sent.

A preferred feature of these additional credit card numbers is that they be constrained to be in the correct format for a credit card number with a valid check sum, while at the same time be mathematically unrelated to each other or to the master credit card. In certain situations, for single use numbers, the expiration date is virtually irrelevant. Thus, using the month code of the expiration date with said eleven digits, there are 12×10^{11}, i.e., 1.2×10^{12}, i.e., 1,200 billion possible unique codes available for any given credit card provider. This would allow for 50 transactions a month for 10 years for 200 million account holders, before any codes would have to be recycled or a new header code introduced. When it is understood that there are then another 10^4 header numbers that a credit card provider can use, it will be appreciated that the structure

and arrangement of existing master credit card numbers is sufficient to operate this invention with the advantage that the existing infrastructure of dealing with credit card transactions can be used with minimum modification. All that is required for the credit card provider is to store the generated numbers against the master credit card number or other type of account number.

If, for example, the card is a VISA® card, there are approximately 21,000 issuing banks. The sixteen digit number has a "4" followed by a five digit code to identify the card issuer. The last number is a checksum to verify that it is a valid number. As a result, there are $21,000 \times 10^9 \times 12$ (252 trillion) unique numbers and associated expiry months. This number of codes is sufficient for 36,000 years of transaction processing at the current annual rate of approximately 7 billion transactions per year.

While existing credit card formats allow for a sufficiently large number of available card numbers, numbers will eventually need to be recycled for allocation. As the range of available numbers reduces in size over time, additional or recycled numbers should be added back into this range to ensure that the allocation process is performed from a range sufficiently large to maintain random allocation. The length of time prior to recycling depends on the total number of available unique card codes available to an issuer and the number of transactions that use limited use numbers. Such recycling can only occur after a number has been invalidated for further use and is no longer valid for refunds. Once recycled, automatic fraud detection mechanisms that would normally be activated on the attempted reuse of a previously inactivated card need to be altered by removing the recycled number from the list of previously issued limited use numbers.

The use triggered condition subsequent limitations placed on limited use card numbers, i.e., transaction value limitations, number of transactions limits, etc., are central to their additional flexibility and security compared to conventional credit/debit/charge cards. These limitations can be imposed and controlled in a variety of ways. For example, the limitations can be stored within a database held by the card issuer and used to check that the transaction falls within these limitations during the

authorization process.

Fig. 4 is a flow chart illustrating an exemplary process for limiting the use of a credit card number. A CPU can allocate a credit card number to a master credit card number (step 402), and allocate a condition to the credit card number. (Step 404). The CPU can then store the condition in a database of conditions. (Step 406). These limitations can be assigned by the issuer in a predetermined manner or can be imposed according to the requests of the card holder. These limitations can be encoded with the limited use numbers when the numbers are issued to a user so that the user can determine the limitations associated with a particular card. These limitations can be altered once a number is issued by updating the issuer database and the user maintained list of numbers. Communication between the user and card issuer to make these changes can be posted, conveyed verbally or electronically. (Step 408). When the card is used for a transaction (step 410), the transaction details are compared by the processing software with the limitations and the transaction is authorized only if the transaction falls within these limitations. (Step 412).

Alternatively, the limitations can be encoded within part of the number format that is transmitted during a transaction. The limitations would then be decoded from the transmitted transaction details by the card processor. This would offer the user more control, but would offer less security since knowledge of the encoding format could be used to fraudulently alter the limitations chosen by altering the appropriate portion of the limited use number format.

As Internet commerce develops, there will be an increased need for a wide range of financial transactions. The limitations placed on limited use card numbers can be used to implement a wide range of payment options. For example, a credit card number can be limited to a single transaction for a pre-arranged transaction limit. Or alternatively, a credit card number can be used, for example, to implement an installment plan where the credit card number is, for example, only valid for twelve payments for a pre-arranged transaction limit for twelve months to a single merchant. This plan provides security against fraud because it is locked to a single merchant,

and it is only good for one year. Or similarly, a credit card number can be used to implement a debit plan where the credit card number is limited to a specific merchant.

When the limited use number is limited to a specific merchant, the merchant can be prearranged by the user or can be determined by first use. In this situation a limited use card can be used to generate an account specific to a single merchant. For example, this can be used in situations on the Internet where a web merchant will retain a credit card number for later purchases. By being limited to a single merchant, theft of the number from the merchant's computer systems will not allow the card to be used elsewhere. Also, any such use will immediately identify a specific merchant as having suffered a security breach. Determination-by-first use could involve linking the merchant name or credit card system identification number at the time of making the purchase, during the authorization process or during the settlement process.

Or finally, a credit card number can be used as a gift voucher where the credit card number is limited to a specific transaction value or limit, but it can be used for any merchant. A gift voucher limited use card could also have a pre-determined limitation to a specific merchant or a type of merchants or to a group of merchants such as within an "online shopping mall".

The next matter that is considered is how these additional credit card numbers and/or additional credit cards are distributed to a credit card holder. One way of providing such additional credit card numbers and/or additional credit cards is to in some way provide them physically to the master credit card holder, whether it be by collection, delivery by courier, post or some other way which can generally be covered under the heading of provision by post. Obviously, the financial institutions wish to provide the additional credit card numbers or the additional credit cards to the user as efficiently as possible with the minimum risk of the additional credit card numbers and/or cards falling into a third party's hand. While one can never prevent theft, for example, of a credit card from a user, what is important is to ensure that these disposable credit cards and/or credit card numbers are delivered to the user with the least possibility of a third party obtaining either the numbers or the disposable credit cards from the time

they are generated until the time they are physically received by the user.

It is envisaged that there are various methods by which a credit card provider could issue the additional credit card numbers and/or credit cards to the user. One of the simplest ways would be to post them on request. Another way would be for the credit card provider, after receiving a payment of an account or with a statement of an account, to provide a sufficient number of additional credit card numbers and/or additional credit cards to replace the ones used since the previous statement. Particularly, if such statements do not quote the master credit card number or some code number, it would be possible to put in additional checks on the activation of the additional credit card numbers or credit cards. Some form of receipt system could be used. In this way effective theft would be reduced.

Fig. 5 is a flowchart illustrating an exemplary process for distributing credit card numbers. A credit card issuer allocates a master credit card number or more generically a type of master account number to a master credit card or account owner. (Step 502). The credit card issuer then allocates limited use numbers to the master account number. (Step 504). For pre-prepared cards, the card issuer can decide whether to print (or incorporate by some other means such as embossing) one number per card or multiple numbers per card. (Step 506). The card issuer can distribute multiple numbers using a single card (step 508) or distribute multiple numbers using multiple cards. (Step 512).

In either case, it is important that the user can keep track of which numbers have been used. If the card has only one number, an opaque removable cover can be used to cover one or more portions of the card. (Step 510). For example, the opaque removable cover can cover the number portion of the card, so that the cover has to be removed before the card can be used. The act of removing the cover indicates that the card number has been accessed or used.

Or alternatively, an opaque removable cover can conceal a message such as "used." The opaque removable cover can be a scratch off layer that is scratched off before or

after the card is used. The scratch off layer can resemble the layer that is often used to cover lottery numbers or the like. Or alternatively, the single use cards can be placed in a self-contained container that resembles a razor blade dispenser. (Step 516). The owner can remove a single use card from a first compartment and then place the used card into a second compartment.

If the card has multiple numbers, the owner can keep track of the numbers by using a device that covers one or more portions of the card. (Step 510). The device can cover the numbers until they are used. As described above, the device can comprise multiple opaque layers that must be removed prior to the use of each number. Or alternatively, each number could be visible when the card is issued and each number is associated with a panel in which an opaque covering conceals a message that indicates that the number has been used. After each use, the corresponding covering is removed or scratched off to indicate that the number has been used.

In both above cases the solutions incorporated on the cards act to remind the user which numbers have been used. The critical check on the validity of the number is performed by the processing software responsible for authorizing card transactions.

The additional credit card numbers and/or cards can be sent with a statement. (Step 518). The additional credit card numbers are not activated until the statement is paid. (Step 520). The card issuer could also require that the payment be accompanied by the master credit card number or another identifier. Or, for example, an additional security step involving either direct contact with the issuing credit card company or an independently issued password to allow activation of an electronic device could be used.

A further way in which the additional credit card numbers and/or additional credit cards could be distributed to the user is by way of an ATM machine. (Step 522). The ATM machine with very little modification could provide the additional credit card numbers. Similarly, with relatively little modification, an ATM machine could provide additional credit cards.

Cards/single use numbers can be issued directly into an electronic device that is capable of storing such numbers. This applies to mobile phones and pager devices to which information can be transmitted using existing systems and computers connected either directly or via a telecommunications system to the Internet or a specific host computer system. In such a situation a mechanism is required to protect these numbers in transit to prevent unauthorized access. For global applications, this mechanism must not be subject to export restrictions. In addition, this protection should not be susceptible to "brute force" decryption techniques. Such a system is described below in relation to the storage of single use cards.

An alternative method to provide additional credit card numbers could be by way of a computer programs. Obviously it would be necessary for the credit card provider to have sufficient security that when the computer program was dispatched, either through the telecommunications network or through the post, that unauthorized access could not be obtained.

In the situation where the user stores and accesses limited use numbers via an electronic device such a computer of any form (desktop, television or cable linked Internet access device, laptop, palmtop, personal organizer, etc), any device that can deliver the same functions as a computer or dedicated Internet access device, a dedicated microprocessor device with key pad and screen or any form of telephone with associated microprocessor controlled electronics, the associated software can perform some or all of the following functions:

1) Password controlled access to software or other security activation system that can verify that the user has a valid right of access.
2) Secure storage of issued limited use credit/debit/charge card numbers until required by the user. These numbers can be stored in a variety of encrypted forms. An additional security step is to encrypt the number in the form a valid credit card number as previously described.
3) Secure storage of transaction details and date of use for reconciliation with

records held by the credit/debit/charge card company in case of disagreement. This may include digitally signing each transaction record.

4) Facility for user to review past usage of limited use card numbers and transactions.

5) Notification to user of available number of limited use cards.

6) Initiate automated request from software to card issuing organization or agreed agent for further cards to be issued by previously agreed route if requested by user or if the number of available limited use cards is less than a pre-arranged limit.

7) Secure communication between software package and card issuing organization or agreed agent for downloading additional limited use numbers. This secure communication can exploit any available form of encryption suitable for this purpose.

8) Secure communication between card issuing organization or agreed agent and the software package for the transmission of information regarding credit card transactions, account balances and other information as requested by the user or card issuer. This secure communication can exploit any available form of encryption suitable for this purpose.

9) Automated or manual means for transfer of credit card information to the merchant. The software can integrate with Internet software in the situation where it is run on a device linked to the Internet or similar electronic network and allow automatic transmission of transaction details if the merchant software so allows. To ensure compatibility with any form of merchant software the user also has the option of dragging and dropping a limited use number displayed by the software onto the appropriate part of a web page, or manually entering the number. In the case a device intended for use over the telephone, the number can either be spoken by the user or appropriate tones can be generated to automatically transmit the number to the merchant.

10) Use of digital signature verification to verify both parties of a credit card transaction (i.e. merchant and cardholder).

11) Use of digital signature verification to verify both parties of a communication involving the transmission of financial information or additional limited use card

- numbers (i.e. card issuer and cardholder).

12) Use of stored lists of limited use numbers held by user and card issuer as dynamic passwords to verify both parties (user and card issuer) of a communication involving transmission of financial information or additional limited card numbers.

For "card not present" transactions, it is proposed that the customer uses an electronic device to store issued single use numbers. This may represent a range of devices from a mobile telephone, pager, dedicated single use storage device or a software package that can run on range of platforms such as a conventional desktop computer, television based Internet access device (e.g., WebTV) or a portable computing device.

The software that is used within these devices for storing and accessing these numbers will have specific features that are common to all platforms/devices.

For security reasons, access to the software will be password protected or protected by another security system that allows identification of the user (e.g., magnetic stripe card reader, chip card reader, electronic token generator, fingerprint recognition system or the like). Multiple passwords may be employed to provide limited access to certain individuals, for example limiting access for a family member to single use numbers with specific pre-allocated limits on application or maximum transaction value.

The single use numbers are preferably stored in a secure form involving one or more encryption systems. It is proposed that a dual system will be employed using a standard protocol (e.g., DES or RSA encryption) and a specific system designed for credit cards as described below.

"Brute force" decryption involves using multiple fast computers and specific algorithms to test large numbers of possible encryption "keys." Success can be determined by seeing whether the result appears in the expected format, for example as

comprehensible English text in the case of an encrypted document. If the encrypted version is in an identical format to the unencrypted version (though with different information) then brute force decryption cannot succeed. This is not a computationally viable option for text but it is possible for credit cards.

The approach is to break down each component of a credit card number and encrypt these with a private password so as to maintain the numerical composition of each component. The end result should be securely encrypted but should not represent another existing credit card account. This can be achieved by constraining the encryption system to convert the credit card header sequence used to identify the issuing bank (usually 4-6 digits) into a currently unused sequence. Since this information will be constant for all cards from the same issuer, this information should be randomized (rather than encrypted) to prevent recognition of a valid decryption solution. Once the rest of the number is decrypted by the program, the appropriate header sequence can be added. The remaining digits excluding the checksum (the last digit) are then encrypted using any private key encryption system that will maintain the same number of digits and produce a result that represents the numerals 0 to 9. The expiration date and any other identifying digits are also encrypted in such a manner as to respect their existing structure, i.e., the month is encrypted between 1 and 12 and the year is encrypted so as to represent a number within the next three years that ensures that the expiration date is valid. Following these steps, the digits used to calculate the checksum in a normal card number are processed to calculate a valid checksum for the encrypted card. The result is a valid appearing credit card number that has a valid checksum and which can be guaranteed not to belong to any existing credit/debit card account holder.

For example, for a card with a 6 digit header and valid checksum, e.g., "1234 5678 9012 3452 expiration date of 12/99," 123456 is randomly assigned to a currently unused header sequence, e.g., 090234 (this is an example and does not necessarily represent an unused header sequence). 789012345 is encrypted into another 9 digit number, e.g., 209476391. 12/99 is encrypted to a valid date format that ensures the card is not expired, e.g., 3/00. The checksum is recalculated to

produce a valid appearing credit card number, for this example the checksum is 4, i.e., 0902 3420 9476 3914 expiry 3/00.

To decrypt this number for use or after transmission from the bank, the appropriate header sequence for the issuer is exchanged for the digits in the encrypted number. The other digits are decrypted using the private password and the check-sum is recalculated.

Provided that the header number is unused and the private password remains private, then this number is encrypted in such a way that brute force encryption cannot be used to determine the original number, since it will not be possible to determine when the correct solution has been reached. In combination with standard encryption systems, this allows a means to securely store credit cards and transmit them over insecure systems with confidence.

Once the appropriate password is entered into the software, the next available single use number is decrypted and either displayed, allowing the customer to use it in any form of trade that can achieved by quoting credit card information, or directly transmitted via the software to the merchant. Once used, the single use number is removed from the stored list. The date of access, the number accessed and any additional available transaction details are then stored in a secure fashion and digitally signed to allow for verification in the case of a disputed transaction. Each access to a single use number requires the entry of a password to prevent unauthorized access if the customer leaves his software/computer device unattended and active.

Other types of encryption may also be used, for example, which require the use of a mask and/or private key. For example, as described above, this approach also breaks down and encrypts each component of a credit card number so as to maintain the numerical composition of each component. Similar to that described above, the bank identifying header sequence, e.g., in the case of VISA ® cards, the initial digit "4" followed by the 5 digit BIN number, is replaced with an equal number of random digits taken from the range of unused headers. This ensures that the resulting number does

not represent some other valid existing credit card number. These replacement header sequence digits can be fixed for a given card issuer and can be reconstructed after decryption.

The final checksum digit can be handled in one of several ways. For example, the checksum digit can be recalculated based on the encrypted remaining digits as described above. Alternatively, the final checksum digit can be omitted from the encryption process and recalculated after decryption.

The remaining digits can be reformatted into another number with the same number of digits by any reversible encryption process. The same process may also be applied to all other numerical information transmitted that may be issued during a transaction, e.g., the expiry date and other codes. One process for randomizing these remaining digits is described above. Another process to encode the remaining digits is to perform a digit by digit mathematical operation in combination with a mask containing the same number of digits as the remaining digits to be encoded.

For example, assume the original remaining digits are 878918982 and the random mask digits, containing the same number of digits as the remaining digits to be encoded, are 143337658. A modulo 10 arithmetic function is then performed using the original remaining digits and the random mask digits as follows to achieve the encrypted result.

Original remaining digits	8	7	8	9	1	8	9	8	2
Random mask digits	1	4	3	3	3	7	6	5	8
Encrypted remaining digits	9	1	1	2	4	5	5	3	0

After transmission of the encrypted card number, including the replacement header sequence digits, the encrypted remaining digits and the checksum digit, if appropriate, the encrypted card number is separated out into its components. The encrypted remaining digits are decrypted in the opposite manner in which they were encrypted.

Specifically, knowing the random mask digits and the encrypted remaining digits, a modulo 10 subtraction is performed to reconstruct the original remaining digits as follows.

Encrypted remaining digits	9	1	1	2	4	5	5	3	0
Random mask digits	1	4	3	3	3	7	6	5	8
Original remaining digits	8	7	8	9	1	8	9	8	2

Even with this simple encryption technique, the decryption solution requires access to the private key because the solution cannot be identified in isolation. In addition, this process enables the reconstruction of one of the sequences, i.e., the original remaining digits, the random mask digits or the encrypted remaining digits, knowing the two other sequences.

Fig. 6 is a flow chart illustrating an exemplary process for electronically using credit card numbers. The software can be launched either on its own or activated by an icon integrated into an Internet browser. (Step 602). The software can provide a simple interface with a graphical appearance that exploits familiar images of credit cards and/or ATM's. The software can be programmed using Java code or a Java core embedded in a c/c^{++} application or equivalent programming language.

Once launched the user puts in one password to gain access to the main screen which contains a key pad to allow a PIN to be inputted either by keyboard or by mouse clicks. (Step 604). The latter protects against any covert attempts to record passwords by trapping key strokes. A consecutive number of errors in inputting the password will permanently disable the program and overwrite remaining encrypted numbers. After the correct PIN is entered, the user can select a new limited use number with or without additional constraints (e.g. maximal transaction value). (Step

606). A new limited use number is then displayed on the graphical interface. The software can provide secure access to encrypted credit card numbers that are stored on a computer's hard disk. (Step 608). These numbers can be accessed for use on the Internet or for use over the phone/mail order. (Step 610). The numbers must therefore be able to be inserted directly into a web page (step 612), or printed out/copied from screen for use in other ways. (Step 614). The limited use number can be copied, printed, pasted via the clipboard (or equivalent) or dragged-and -dropped onto a web page. The length of time a number is displayed and how the program terminates are user configurable. The user can also record a comment to provide further information about how a number was to be applied. For automated transactions, the software should ideally be able to intercept and respond to merchant server initiated signals activating integrated functions within the browser.

Once a number has been accessed, it can be deleted from the encrypted lists. (Step 616). The date, number, current URL in the case of Web use and any user comments are then stored by a separate form of encryption to facilitate audit/review. (Step 618). The user can review, but not edit this information

There should be a facility for downloading additional numbers either from additional floppies or via the Internet using high security protocols. (Step 620). The latter function can be performed by a separate program.

The program should include a maximal degree of transparent security features, i.e., features that do not affect a normal user, but that protect against the program being reinstalled or copied onto a second machine. This means that the encrypted limited use numbers should either be stored within the executable file or stored in a file that also stores encrypted copies of the machine specific information. (Step 622). This is required to ensure that the numbers can only be accessed on the machine on which the software was first installed. The data files should also be stored as hidden system files.

Some users may wish to have the equivalent of an electronic wallet that can be de-installed from one computer and reinserted on another, for example, when transferring a "wallet" from an office to a home machine. This transfer process ensures that only one version of the program is running at any one time and that no problems arise in terms of reconciling lists of used numbers. Appropriate security mechanisms can be implemented to identify the valid user.

Appropriate security measures include encryption. Encryption of limited use numbers should involve two levels as exemplified above. At the first level, the card numbers are encrypted using an algorithm that acts only to alter the free digits within the credit card. The header sequence (i.e., BIN number) is left unaltered or converted into an unused BIN number and the checksum recalculated. This prevents any form of brute decryption because there will be no way of telling when the correct algorithm has been selected since each number starts and ends up as a valid looking credit card number. Following this step each number is encrypted with industry standard encryption methods (e.g. RSA or DES). Following decryption within the program the checksum is recalculated for the final number and the appropriate bin number reinserted.

The software can be shipped on a single 1.4 Mb Floppy (or any other computer readable or usable medium) in an encrypted form or downloaded from a website. Limited use numbers can be issued either with the program or independently. An independently shipped password can be required for installation. The installation process will allow the program to be installed a restricted number of times after which critical data is overwritten. The precise number of allowable installations will be easily alterable within the software design. Once installed on the host computer, the program encrypts internal information regarding the machine's configuration to protect against copying of the program onto other machines. At first installation the user can select his own passwords. These will be used to control both access to the programs and to influence the pattern of one level of encryption that is applied to limited use numbers.

As numbers are accessed, a graphical indicator of the remaining amount of limited use numbers provides early warning if additional numbers are required. The software can also provide a log of previously accessed numbers, the date, associated URL if activated from within a browser and comment; a summary of account expenditure; assistance with adding additional numbers from disk or via Internet; the ability to configure additional passwords/users for shared cards; and/or hot link Internet access to the card number issuer's web site.

It is envisioned that additional credit card numbers and/or additional credit cards would be processed by merchants in the same manner as existing credit card numbers and/or credit cards with the merchant obtaining validation of the credit card number from the credit card company or authorized third party. In much the same way as at present, the additional credit card number would be matched to the customer account and the account would be debited accordingly. The merchant reimbursement following verification of an additional credit card transaction would be performed in the normal manner. A particular advantage for the merchant is that since they are never in possession of the master credit card number or indeed, in many instances, of the master credit card, they have no responsibility for security to the master credit card holder. It is envisaged that where there are additional credit cards used, it may not be preferable to take an imprint of the credit card manually, as the imprint can be taken electronically. Similarly, those processing the credit cards will process them in the same manner described heretofore.

Processing systems for handling limited use cards perform a number of functions including some or all of the following:

1) Verify that the limited use number is valid.

2) Verify that the transaction falls within limitations placed on the specific number.

3) In the case of a limited use number associated with another account, verify that transaction falls within limits acceptable for the associated account.

4) Provide authorization to the merchant if valid and within the limitations for specified number and associated account.

5) Permit later transactions to be charged to a limited use number that has been invalidated for further authorizations only if the transaction is generated by the same merchant that obtained pre-authorization for the same transaction.

6) Deny authorization if invalid or exceeding limitations on number or associated account.

7) Activate fraud detection mechanisms if invalid number or on attempt to reuse an invalidated limited use number.

8) Invalidate limited use number for further authorizations/payments if limitations on use are met or exceeded by a specific transaction.

9) Maintain list of invalidated numbers for reimbursement in the case of returned or faulty goods for a defined period.

10) Limited use numbers and transaction details logged and linked to associated account.

11) Transmit records of limited use and other card transactions to the user by post or e-mail.

12) Instigate payment to merchant for approved transactions.

13) Instigate reimbursement to account holder in case of a refund.

14) Invoice account holder for payment for charges incurred or arrange settlement via another account.

Many of the procedures associated with limited use cards represent functions already performed by the clearing systems. These existing functions include: adding new credit/debit card numbers to the processing databases; allowing these card numbers to be activated following a confirmatory call to the issuer by the customer; conferring a credit limit on a credit card number; and invalidating a credit card number from further use and marking any further use as fraudulent. This overlap represents part of the commercial value of the single use invention, minimizing the required changes.

Once a limited use number enters the clearing system it can be handled in a normal fashion, e.g., by ensuring that it has not been reported as being stolen and that it represents a valid account number within the database. If the transaction is within the credit limit of the customer and the transaction limit or restricted use limitations of the limited use number, it is authorized.

Several specific modifications should be made to the processing software to implement the features of limited use cards. For instance, valid limited use numbers are stored in a database of valid account numbers along with other information specific to limited use numbers. This includes sufficient information to identify the customer to whom it was issued and any additional limitations placed upon the card in terms of transaction value or category of merchant for which the card can be used.

Once authorized, the limited use number is invalidated so as to ensure that further authorization/charges cannot be made on that number. To allow for authorization preceding request for settlement by a substantial delay, for example in the context of a mail order purchase where a credit/debit card number may be authorized at the time of order and charged only when the product ships, delayed settlement to the same merchant must be allowed.

Once the number of transactions permitted for a limited use card is reached, the central card processing software invalidates the card. Due to the time delay that can occur between authorization and a merchant request for settlement, improved security

is achieved by linking the invalidation process to authorization. Linking invalidation to settlement facilitates pre-authorizations at the cost of increased risk of, for example, multiple use of a card number intended for limited use. Pre-authorizations can be used with authorization dependent invalidation as described above. In the case where a transaction is not authorized before being accepted by a merchant, the invalidation process will occur when the transaction details are transmitted to the processor for settlement. When no authorization is obtained for a limited use number the system will therefore still operate normally with an increased level of risk for the issuer/merchant as is the case with an unauthorized conventional card transaction.

Whenever the credit limit or validity of a customer's account changes, all currently valid limited use numbers are identified and their associated credit limit is altered to the lower of either their allocated transaction or the existing credit limit. If the customer account is closed or declared delinquent, all valid single use numbers are handled in the same manner.

Whenever a limited use number is used, the next available single use number previously allocated to the same customer and issued to the customer is added to the database of valid account numbers.

When a transaction is charged to a limited use number, the transaction details and customer account details are stored together for audit purposes and the value of the transaction is added to the customer's account for billing.

The software for storing transaction details and printing statements can be modified to allow for both the customer's conventional account details and the limited use number transaction details to be reported.

Processing of limited use numbers can be integrated into existing systems in a variety of ways. The authorization and settlement process can be completed in a single cycle or split into a separate authorization and settlement processes as is commonly done in existing credit card systems.

In the case of an entirely new, stand-alone, limited use credit/debit/charge card processing system, the above functions can be implemented without restriction in any suitable computer capable of incorporating the required database and communication functions. Such a system should be able to provide an authorization for a transaction within the same time scale as an existing credit/debit/charge card transaction.

In the case where the above functions have to be integrated into existing systems several approaches can be taken to minimize the required changes. It is possible to add steps to the processing chain that is encountered as soon as a credit/debit/charge card number is received from a merchant.

Fig. 7 is a flow chart illustrating an exemplary process for processing a transaction. In step 702, a software system receives transaction details from a merchant. The software system determines whether the number is a limited use number or a conventional card number. (Step 704). If the number is a conventional card number, it is passed on unchanged into the processing system and can be handled by existing systems with no modification. (Step 706). The merchant receives authorization from the system responsible for authorizing conventional card numbers. Merchant reimbursement is similarly unaffected. (Step 708).

The system can check the limited use number and the corresponding limitations. (Step 710). If the number is not valid for the designated transaction, the transaction is denied. (Step 712). Otherwise, a database look-up procedure determines the associated master account number and transmits this number (i.e. the master account number) back into the processing system. (Step 714). This allows all existing fraud detection, authorization and demographic software procedures to be completed with no alteration. (Step 716). Once the master account number is substituted for the limited use number a number of additional steps are required. (Step 718). If the criteria for invalidating the limited use number have been met during this transaction, then the limited use number is invalidated for all future transactions except refunds. An additional limited use number can be automatically issued if a continual supply of

single use numbers is required. The transaction details and master account number are then transmitted for inclusion within a database to allow for tracking of transaction details and billing of the user. These functions do not need to be performed before an authorization is issued but can completed afterwards. (Step 720). However, performing such steps together with the validity verification of the limited use number prior to issuing an authorization message to a merchant is a feasible option with a minor reduction on the processing time required to issue an authorization message.

With the above system, the software responsible for substituting the master account number for the limited use number can also process additional features unique to limited use numbers. These features include transaction value limitations, merchant type restrictions and geographical limitations. If the transaction exceeds the limitations placed on the limited use card then authorization is denied and the master credit card need not be passed on for further processing. In the case of a transaction falling within the limitations of a limited use card, then the transaction details are passed on with the master account number for conventional validation. In this way the restrictions in place for the master account (e.g., available balance, expiry date) are checked for each limited use transaction.

Specific fraud detection mechanisms can also be incorporated into the software. For example, on the first occasion that an invalidated limited use number is used this transaction can be flagged as potentially fraudulent and appropriate measures taken. Repeated attempts to authorize invalid numbers from a single merchant or group of merchants also potentially points to fraud and can lead to activation of appropriate fraud management measures.

The above system requires the least modification of existing systems but may take up to twice the processing time of a conventional transaction due to the double authorization process, once within the limited use verification and translation step and once within the standard systems. It may be advantageous to initially process the limited use card as a master credit card by using a single list of limited use numbers and master credit card numbers.

Fig. 8 is a flow chart illustrating another exemplary process for processing a transaction. In step 802, a software system receives transaction details from a merchant. The software system has access to a database that contains additional information to identify the associated account or means of settlement and specific limitations relating to the use of limited use cards. As a result, limited use numbers can be associated with existing accounts in the manner currently used to associate multiple conventional accounts in the case of multiple cards issued to a single company for corporate use. (Step 804). During an authorization the associated account number need not be identified provided each limited use account is updated whenever the status of the associated account changes (e.g. available balance, account validity etc.). The system can deny authorization (step 806) or authorize a transaction (step 808) without identifying the associated account number.

For settlement and billing purposes (step 812), the associated account needs to be identified (step 810), but this does not need to be done during the course of an authorization. The existing software should be modified or linked to a new program that performs duties specific for limited use card numbers as described above. (Steps 814, 816, and 818). These functions do not need to be performed before an authorization is issued. These functions can be completed afterwards.

This system requires more modification of the existing processing software systems, but offers authorization times within the same timescale as existing transactions since only one authorization steps is involved. Other activities such as updating the limitations on the limited use card when the master account changes can be performed outside the authorization process (i.e., "off-line").

Such other activities can also take place while the system is operating. The system may include some or all of the following features:

1) A system capable of altering the nature and value of limitations associated with a specific limited use credit/debit/charge card number on the basis of the

— usage of that specific limited use card number in transactions, where such alteration is conducted while the system is operational;

2) A system capable of altering the nature and value of limitations associated with a specific limited use credit/debit/charge card number on the basis of instructions generating on behalf of the issuing bank, where such alteration is conducted while the system is operational; and

3) A system capable of altering the nature and value of limitation associated with a specific limited use credit/debit/charge card number on the basis of instructions generated on behalf of the card holder, where such alteration is conducted while the system is operational.

The invention is not limited to the embodiments hereinbefore described but may be varied in both construction and detail. For instance, the invention has been heretofore described mainly in the context of a system in which a customer receiving a single use card already has a main account with the credit card provider. But this need not be so. For example, it is envisaged that an ATM machine (or similar apparatus) could be used by people who did not have a credit card account to purchase disposable credit cards, which disposable credit cards could then be used for either card present or remote transactions. When the card had been used, the card would be simply reinserted into the ATM machine, and after a suitable period of time the purchaser's account would be credited with any money not spent. Similarly, if the person who purchases the disposable credit card does not have an account of any sort with the credit card provider, the credit card could still be purchased from the ATM machine and then any refund could take place a sufficient time after the transaction would have been cleared, which refund could be either in the form of a cash refund to the purchaser or to a crediting of that purchaser account with another financial institution. Similarly, it will be appreciated that the use of an ATM machine is not essential, as the disposable credit cards or single use credit cards could be purchased in the normal way in which one purchases any other goods or services, such as either directly in a face-to-face transaction or by post.

Similarly, while in the above it has been suggested that there could be single use credit cards that would be purchased, there is no reason why they could not be multiple transaction credit cards with an aggregate credit limit. Further, these cards could, instead of being credit cards, be simply credit card numbers for single or multiple use. It is, however, envisaged that for operational efficiency, these numbers are much more likely to be issued as disposable credit cards or single use credit cards. Thus, for those who do not wish to handle a credit card or whose credit worthiness is such that they would not be allowed to have a credit card, it will now be possible for them to have the use of a credit card. This would have considerable advantages for the credit card providers.

In processing a transaction as described above, one step is to determine whether or not a limited use credit/debit/charge card number is valid. As discussed above, when a new credit card is presently issued, it is commonly required that the card holder activate the card. Specifically, the card holder may be required to communicate with the credit card issuer to activate the card before it can be used. Alternatively, in one embodiment of the present system, the card holder can control the activation or validity of a credit card number, or equivalent transaction code, during the course a transaction. Thus, in this embodiment, the card holder has the control, security and confidence that payments can only be made with his or her express permission.

Fig. 9 is a flow chart illustrating an exemplary method of controlling the validity of a limited use credit card number. The card holder has a credit card number, or equivalent transaction code, that is allocated to the card holder, but is not yet active. (Step 902). The card holder can acknowledge delivery of the credit card number, but the number remains inactive within the card issuer's processing system, e.g., a bank's processing system. (Step 904). When the card holder wishes to conduct a transaction, he or she contacts the card issuer to activate the credit card number. (Step 906). Activating the credit card number before every transaction is cumbersome, but in the context of a remote transaction for example, via the Internet or equivalent network, the communication between the card holder and the card issuer can be achieved very rapidly by an entirely automated system that will activate

the card during the process of conducting a transaction with an Internet based merchant. The credit card number is activated for a specific transaction only when specifically requested by the card holder. (Step 908).

The properties of this validation or activation process can vary. For example, the validation could be for a specific time period, for a specific merchant or group of merchants, for a specific type of transaction, or for a specific number of transactions (authorizations and/or presentments). These properties can also be combined in any permutation. For example, a card holder could request that his or her credit card number be validated for one transaction with a specific merchant up to a specific value limit or value range (e.g., a specific value +/- a configurable range). In the event that no authorization is received within a defined period, the validity can lapse. This combination provides a solution that meets the need for a secure, flexible payment system for remote transactions.

More specifically, for Internet transactions the card holder would receive a software package from the card issuer along with a unique personal validity limited credit card number. This software package would also facilitate completion of the merchants web page using ECML (electronic commerce modeling language) or some other equivalent electronic wallet system. Merchants wishing to use this system provide a unique merchant identification number on their web site. For merchants who are not compliant with such systems, a simpler automated method, e.g., "drag and drop," of transferring card number and other details is supported.

When a card holder wants to conduct a transaction, he or she activates the validity limited credit card software using a password or hardware based user identification system (e.g., magnetic stripe card reader, chip card reader, electronic token generator, fingerprint recognition system or the like) thereby identifying himself or herself with the card issuer. The card holder then requests his or her credit card number to be validated for the merchant as identified by the merchant identification number. After use the card number is automatically inactivated again. The card holder may also specify additional limitations as discussed above, such as value

limitations and maximum number of available transactions. Alternatively, these limitations could carry default limitations, for example single transactions up to a value of $100.00. This request would be transmitted via the Internet to the card issuer's card computer processing system. The processing system would validate the card holder's password (or hardware device), if appropriate, and forward the appropriate validity request to the card processing systems database.

The card issuer's server may also verify the merchant's identity by providing confirmation of the merchant's name as it will appear on the card holder's credit card statement. This merchant verification helps to avoid a common source of potential confusion for card holders in credit card transactions. The merchant identification number can either be the actual credit card systems merchant-ID or another unique code. In either case, the credit card merchant-ID that will be transmitted to the processing system during the transaction is entered into the processing system's database. This ensures that only the intended merchant can initiate a transaction with the validated credit card number. In the event that a merchant identification code does not satisfy the card holder's expectations, the card holder has the option to cancel the transaction before any information is passed to the merchant's web site.

When application of the one or more limitations are confirmed, generally within a matter of seconds, the card holder is given verification of such and is allowed to transfer the credit card number and transaction details to the merchant's web site. Since the merchant identification number is used to validate a specific number of transactions for that merchant, there is no benefit of a rogue or fraudulent merchant trying to steal the identity of another valid merchant. The transaction can only be reimbursed to the merchant identified to the card holder by the card issuer's system.

When a merchant receives the card holder's credit card number, the merchant processes this in an identical manner to an existing transaction in known systems. The transaction is passed through to the card issuer's processing system via the merchant acquiring and credit card networks. At the card issuer's processing system, the transaction is handled by an authorization system that allows a card number to

have associated validity restrictions or limitations, such as merchant-ID. If, in response to an authorization request, the authorization system indicates a valid card number, with an appropriate merchant-ID validation and sufficient funds, a normal authorization response is returned to the merchant. The number is then deactivated by the use triggered processing software within the authorization system or the in case of a multiple outstanding transactions the properties of the card number are updated to remove the permission for the authorized transaction (e.g. decrement the cumulated value limit). If the authorization system identifies a problem with the request, for example, exceeding a limitation, the merchant is denied authorization. Transaction settlements and card holder billing proceed as described above.

In the situation where a card holder is making multiple purchases with the same merchant within a short period of time, each validation by the card holder may be cumulative so that all the requested transactions can proceed. For example, if the card holder requests two transactions, one of $50.00 and one of $100.00 dollars for a specific merchant, the credit card number will be validated for two transactions to that merchant with a cumulative limit of $150. This means that both transactions will be authorized. In this case, the sequence of authorization requests from the merchant may differ from original sequence of validation requests from the card holder.

This system may be implemented using the internet card software package, or RAD software package, as described herein.

In general, the system provides a method for numbers and accounts to be set up and issued directly to the user. In addition, the system also permits users to directly alter the properties of a credit card account within an issuer's authorization and settlement system. The set-up (issuance) and use of a limited use credit card number can take place at the same time, i.e., in the same interaction or at separate times, i.e., setting up (issuing) a limited use credit card number at one time and configuring the limited use credit card number at a later time.

This system has a number of advantages over existing credit card systems. Card

fraud is greatly reduced since a stolen number requires the card holder to validate the card number before any transaction can be completed. This protects against either interception of the number during a transaction or the number being accessed from a merchant's computer systems at a later date. In addition, if the number is authorized, the merchant is assured that the card issuer has directly validated that the card holder has requested the transaction. This prevents or limits a card holder's ability to repudiate the transaction. Moreover, the card holder has additional control on the purchasing power of his or her credit card. The card holder has the reassurance that payment can only be made to the merchant described by the card issuing bank/organization.

In situations where the card-holder and card issuer are in communication and authentication is required of one or both parties, the list of limited use card numbers held by each party can used as a form of identification. In the manner of a dynamic password all or part of a single limited use number a sequence of such numbers could be used to identify either party without the need for issuing any additional security systems. Since this identification does not need to be handled by conventional transaction systems, all or part of a limited use number can be used for this purpose.

Fig. 10 is a flow chart illustrating an exemplary process for using a credit card number as a PIN number. In step 1002, a card issuer generates a database of available credit card numbers. The card issuer selects a master credit card number or more generically master account number (step 1004) and distributes the master account number to a master account number owner. (Step 1006). The card issuer then allocates additional credit card numbers to the master account number (step 1008), and distributes the additional credit numbers to the master account number owner. (Step 1010). When the master credit card number owner needs or desires to access account information (step 1012), the master account owner can use one of the additional credit card numbers as a PIN number. (Step 1014).

As can be readily seen, there are fundamental differences between the system of the present invention and any system that uses a PIN or other number (whether constant

or varying from transaction to transaction) to validate a transaction. In the present system the numerical details conveyed in the course of a transaction are identical in format to an existing credit card number but no unique account code is included. This maximizes the security and privacy of a credit/debit/charge card transaction. Within the processing system the validity of the limited use number is verified first and then the associated account identified second by examining information stored with the limited use number. With the transmission of an additional PIN or other number in addition to the account number or other unique identifier, there is a lower level of security and privacy. Within any form of PIN identification (and as described by Rahman) the associated account is identified first and then the PIN verified after this step. For this reason many card holders can share the same PIN, indeed in most cases due to the short length of PIN codes many users do have identical PINs but different account numbers. For our system each limited use number must be unique at the time of use and so the associated account can be uniquely identified.

With reference back to Fig. 1, and as described above, central processing system 100 can internally perform the approval and denial of credit card transactions or this function can be delegated to a separate clearance processing facility. In other words, central processing system can be located within the card issuer's main processing system or at a stand-alone facility. In an exemplary embodiment of the present invention, central processing system 100 adds additional functionality to existing credit/charge/debit card systems without any, or with minimal, alterations. In general, central processing system 100 transmits certain transaction details in a bi-directional manner, i.e., utilizing dual interfaces between central processing system 100 and the merchant and between central processing system 100 and the card issuer, without revealing the master credit card number to the merchant. The dual interface transmissions, referred to herein as remapping, allow merchants and card issuers to handle transaction details in the same manner as conventional credit card transactions. Such conventional credit card transactions may be, for example, authorizations, settlements, copy requests, and charge-backs.

Remapping can be implemented by utilizing database look-up functions using existing industry-standard computer platforms. In addition, remapping may occur by replacing the limited use card number with the master account number.

Fig. 11 is a block diagram illustrating a credit card system 1100 in which a central processing system 1106 in accordance with an embodiment of the present invention is located within a card issuing bank's main processing system 1114. System 1100 includes merchant acquirers 1102 connected to card issuing bank's main processing system 1114 via credit card network 1104 and switch 1116. Credit card network 1104 may be any type of communication network, such as the Internet, a radio network, etc. as described above. Switch 1116 includes hardware and software components. Switch 1116 may be configured to direct incoming transaction details on the basis of the card number and to direct outgoing transaction details on the basis of the merchant acquirer identification number (referred to herein as the "merchant ID").

Issuing bank's main processing system 1114 includes issuing bank processing facility 1112 and central processing system 1106. Central processing system 1106 includes acquirer interface 1108 and STIP interface 1110.

Exemplary transactions will now be described with reference to Figs. 11 and 12. Fig. 12 is a flow chart illustrating an exemplary method of conducting a limited use credit card number transaction. A user initiates a transaction by presenting a limited use credit/charge/debit card number, either in person or remotely as discussed above. (Step 1202). Merchant acquirer 1102 routes this limited use credit card number to central processing system 1106 via network 1104 and switch 1116. (Step 1204). This routing is done on the basis of a specific bank identification number (referred to herein as "BIN") which is the first few digits of the limited use credit card number, as discussed above. In this example, central processing system 1106 acts as a stand-in processor.

If the limited use credit card number is invalid, or if the limited use condition has been satisfied, i.e., the condition has been met or exceeded, step 1206, central processing

system 1106 will transmit a signal to merchant acquirer 1102 denying authorization of the card number via switch 1116 and network 1104. (Step 1208). If the limited use credit card number is valid, and if the limited use condition has not been satisfied, central processing system 1106 transmits a signal to the issuing processing facility 1112 via merchant acquirer interface 1108 and switch 1116. (Step 1210). This signal includes the original transaction details but the card number and the merchant ID are remapped. This remapping provides the master credit card BIN number so the signal will be routed to processing facility 1112. This ensures that the authorization can be obtained against the master credit card and that any resulting authorization, or denial thereof, is returned to central processing system 1116, as this appears to processing facility 1112 to be the merchant. (Steps 1212 and 1214). The authorization, or denial of authorization, is the remapped within central processing system 1106 to the original limited use credit card number and merchant ID. (Step 1216). Central processing system 1106 then transmits a signal to merchant 1102 authorizing the limited use credit card number, or denying authorization as appropriate, along with the original transaction details via switch 1116 and network 1104. (Step 1218).

Fig. 13 is a flow chart illustrating an exemplary method of conducting a settlement transaction. In a settlement transaction, merchant 1102 transmits a signal to central processing system 1106 via network 1104 and switch 1116 according to the BIN of the limited use card number. (Step 1302). Central processing system 1106 remaps the limited use credit card number with the master credit card or account number, the merchant ID with a central processing system ID and the merchant text description with a central processing text description, step 1304, and transmits this remapped information to issuer processing facility 1112 via switch 1116, step 1306. Processing facility 1112 settles the transaction by payment, if appropriate, to central processing system 1106. (Step 1308). Central processing system 1106 then remaps the master credit card or account number back to the original limited use credit card number, the central processing ID back to the merchant ID and the central processing text description back to the merchant text description, step 1310, and transmits this information along with the payment, if appropriate, to merchant acquirer 1102 via switch 1116 and network 1104, step 1312. As with the authorization cycle, this

settlement cycle ensures that settlement is obtained against the master credit card; that the card holder's billing statement reflects the limited use transaction, with the central processing ID, and that the payment for settlement is conducted through central processing system 1106.

If a card holder challenges or questions a specific charge on his or her billing statement, the copy request or charge back will be routed to central processing system 1106, as this is the ID associated with the transaction. In a similar manner to that described above, central processing system 1106 will remap the copy request or charge back according to the merchant ID and the limited use credit card number and transmit the copy request or the charge back to merchant 1102 via switch 1116 and network 1104. Merchant 1102 transmits the requested copy or the charge back confirmation to central processing system 1106 via network 1104 and switch 1116 according to the BIN of the limited use card number. Central processing system 1106 then remaps the ID and card number information and forwards the requested copy or charge back information to processing facility 1112 via switch 1116.

System 1100 is advantageous in that it reduces communication delays and fees but it requires the addition of switch 1116. Alternatively, Fig. 14 illustrates central processing system 1406 as a stand alone facility. The authorization, settlement, copy request and charge back transactions described above are equally applicable to Fig. 14, except switch 1116 in Fig. 11 is no longer required. Fig. 14 illustrates that communication between central processing system 1406 and card issuing bank's processing facility 1412 can be conducted through existing credit networks 1404. In addition to not requiring a switch, such as switch 1116, in this configuration, a single large central processing system 1406 can offer limited use support to a wide range of issuers, such as bank processing facility 1412. However, this configuration requires increased communication times and potentially increased communication fees.

In another exemplary embodiment, the central processing system could be constructed to be a part of the merchant acquirer, instead of the bank processing

facility as shown in Fig. 11. This configuration would also require the addition of a switch like switch 1116 but would reduce communication delays and fees.

The limited use credit card number and remapping system may also be used in connection with organizations other than banks. For example, the limited use credit card number may be linked to organizations such as utilities, internet service providers, telephone accounts, fixed or mobile, anonymous prepaid accounts and the like. With such other organizations, there would be no remapping to a master credit card number, but rather to some other account number provided by the organization.

Linking a limited use credit card number to other organizations is advantageous for several reasons. First, the organization may have a pre-existing relationship with the user of the limited use credit card number. This relationship provides evidence of the user's credit history with the organization, so no additional credit checks need to be performed, which can be costly and time-consuming for the organization. In addition, because the organization is already providing other services to the user, a billing procedure is already established. The time and cost associated with establishing and implementing billing procedures has already been incurred. Minimal cost and effort is associated with adding a section to a billing statement for a limited use credit card number.

A card holder may desire to access a list of limited use credit/debit/charge card numbers where the limited use cards are not stored on the card holder's own computer. In the context of modern client server architecture this represents one extreme of the situation where all information storage is at the server. The previous description for local storage indicates the situation of a client program with a significant amount of local functionality. Between these two extremes a range of intermediary client server arrangements such as a "thin client" with minimal functionality obtaining limited use numbers from the server as required. The combination of encryption and dynamic passwords, as described herein, or any suitable alternative form of use identification allows a card holder to have "multiple

wallets", i.e., a card holder can access limited use numbers from different devices, without the need to transmit credit card numbers.

As discussed above, software and limited use numbers can be issued via electronic communication media. In one embodiment, a card holder can access limited use credit card numbers during electronic transactions via a Remote Access Device, referred to herein as "RAD", such as the Orbis Internet Card□. The overall layout of the RAD system 1500 is shown in Figure 15 and a flow chart illustrating an exemplary method of providing remote access devices for accessing limited use credit card numbers is shown in Fig. 16. In general, the operation of the complete system from registration to completion of a transaction follows.

When a user desires to register with RAD system 1500, the user submits user authentication information, the master account number and other identifying data for entry into a database 1502. (Step 1602). To register with RAD system 1500, the user must be a valid holder/user of the master credit card o r account number. (Step 1604). Once registered, step 1606, the user obtains a RAD 1504, step 1608. RAD 1504 includes a software package to which enables communication with a remote access device support server, referred to herein as a RAD support server 1506, such as the Nexus User Support Server□, to enable the issuance of limited use card numbers.

When the user initiates communication with RAD support server 1506, step 1610, RAD support server 1506 first authenticates the user, step 1612. If successfully authenticated, the user can then request a limited use number, step 1614 specifying any additional transaction limitations desired as discussed herein, step 1616. RAD support server 1506 issues a request over a network to a central processing station 1508 for a limited use number with the one or more specified limitations. The limited use number provided in response to the request is associated with a specific RAD system user identification previously assigned to the user.

Central processing station 1508 obtains the next available limited use number. (Step

1618). Once obtained, the limited use number, and the specified limitations, is entered into database 1502 such that the limited use number is associated with the user's information already in database 1502. (Step 1620). The limited use number is then transmitted to the RAD support server 1506 for issuance to the user via RAD 1504. (Step 1622). RAD software package 1504 displays the limited use number. The user can transfer this limited use number to a web site for initiating a transaction. Transferring this number to a web site can be achieved by dragging and dropping the number onto the web page, by software-simulated key-stroke entry, by "one-click" methods, or by other suitable methods known to one skilled in the art.

When a merchant 1510 receives a transaction utilizing a limited use number from RAD system 1506, the transaction details are handled in the same manner as an existing number since limited use card numbers share the same format as existing credit card numbers. The transaction details are transferred to the merchant acquirer and then routed onto the appropriate issuer on the basis of the leading digits of the limited use number, i.e., BIN, via central processing station 1508. The BIN is registered with central processing station 1508 to ensure appropriate routing.

As described above, central processing station 1508 verifies the validity of the limited use number and ensures that the transaction meets all specified limitations. If the limited use number is valid and the transaction met the specific limitations, central processing station 1508 enters the master credit card number into the transaction message in place of the limited use number. Central processing station 1508 then transmits the transaction message to the issuer's processing facility 1512 as a normal authorization request. The issuer's processing facility 1512 transmits an authorization for the master card number, if appropriate, to central processing facility 1508. Central processing facility remaps the master card number to the limited use number and the transaction message is transmitted to the originating merchant acquirer and then the merchant. Central processing station 1508 also updates the limitations and validity of the limited use number according to the details of the transaction. The limitation and validity updating is best done following verification of available funds so that a limited use number with a cumulative value limit is only decremented in value if the

transaction can be completed. If limitation and validity updating is done prior to checking for the availability/validity of the linked or principal account then certain updates will need to be reversed in the case of a decline on the linked or principal account. This has a small computational overhead. If the authorization was approved by the issuer's processing facility 1512, the user's purchase can proceed as normal. If declined, a decline message is sent to the merchant.

For settlements, the same routing occurs with all transactions deriving from a limited use number obtained from RAD system 1500.

The above described system will now be discussed in greater detail.

RAD system 1500 may be configured to provide the user with many features. RAD system 1500 enables the user to have multiple and different remote devices from which the user may access RAD support server 1506. In addition, it enables a user to have multiple credit card accounts with one or more issuers and to select from amount these multiple accounts. The RAD software package 1504 enables users to have additional passwords associated with an account if desired. The additional passwords can be used, for example, for children and can have additional pre-defined limitations such as a low dollar transaction limits, e.g., $50.00, or merchant class restrictions, e.g., gas stations.

The RAD software package 1504 includes a simple intuitive interface for the ease of the user, the appearance of which may be customizable without modification to the underlying code. RAD 1504 may use images that relate to the front and back of a credit card to provide key areas of functionality. The back of RAD 1504 includes an interactive panel with a magnetic stripe for providing additional information and/or advertising panels. The interactive panel/stripe area provides for password entry and functional selections. Upon activation, the front of RAD 1504 may be configured to provide additional functions, e.g., those required to initiate an on-line purchase. As discussed herein, supplying information required for on-line purchases can be automated in a number of ways including "clicking and transferring" the information,

"dragging and dropping" the information, or "one click shopping."

In one embodiment, RAD software package 1504 is configured to issue a sequence of paired numbers which are securely issued and activated and/or decrypted by oral or written authorization, such as the communication of a password. These paired numbers include an identifier code and a mask code. In order to retrieve a limited use number, a user at a remote device identifies himself or herself using his or her RAD software 1504 by transmitting the identifier code, such as a dynamic password to RAD support server 1506. RAD support server 1506 compares the identifier code with the particular RAD software package 1504 and accepts, or validates, the identifier code if appropriate. If valid, RAD support server 1506 determines the matching mask code for that identifier code from database 1502. RAD support server 1506 uses the mask code to encrypt the limited use card number as described above, and transmits this encrypted code to the user. RAD software 1504 decrypts the encrypted code using the known mask code and reconstructs the initial digits, the BIN number and the checksum digit. RAD software 1504 then arranges this information and reconstructs the limited use card number.

RAD support server 1506 is an Internet based server that interfaces the RAD 1504 and central processing station 1508. RAD support server 1506 receives requests for limited use numbers from users, validates each user, if appropriate, and supplies and validates limited use card numbers with specific limitations, as requested by each user, if appropriate. Such requests may be processed in any desired order, e.g., first come first served basis. RAD support server 1506 may also be configured to provide for location identification verification, secure delivery of limited use numbers, automated completion of payment fields in a merchant's web page order form, review of previous transactions, access to additional issuer services and advertising. The RAD location identification verification is verifying the physical source of the request for a limited use number, e.g., home, office, ATM machine. This additional identification is evidence to limit a user's ability to deny a transaction. The RAD support server 1508 can be configured to require additional identification of the user if the RAD is being used from a physical source which is unknown to the RAD support

server or which has not been previously associated with the RAD by the user.

To accomplish the above tasks, RAD support server 1506 should have a high bandwidth Internet connection and highly secure firewalls to insulate critical information from undesired access. Communications between RAD support server 1506 and RAD 1504 is may be Internet based. Communication between RAD support server 1506 and central processing station 1508 and database 1502 may be secured via private networks for additional security. In addition, to provide for additional security, RAD support server 1506, central processing station 1508 and database 1502 may be located at the same physical location, for example, the issuer's processing facility or some other facility which meets the standards set for banking processing facilities.

Communication between RAD 1504 and RAD support server 1506 can use industry standard security protocols appropriate to the platform. For example, secure socket layer (SSL) encryption may be used in the case of communication by a personal computer of the Internet. Alternatively, one of the encryption schemes described herein may be implemented alone or in combination with password protection and/or smart card user authentication. Such communication security can be selectable by the issuer. For example, issuers can select what type of communication security they desire from a range of options.

While the foregoing description makes reference to particular illustrative embodiments, these examples should not be construed as limitations. Not only can the inventive system be modified for other card numbered systems; it can also be modified for other computer networks or numbering schemes. Thus, the present invention is not limited to the disclosed embodiments, but is to be accorded the widest scope consistent with the claims below.

CLAIMS

1. A method of controlling the validity of a limited use credit card number in a financial transaction system capable of using at least one limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of the at least one limited use credit card number and which is associated the master account number of a customer comprising the steps of:

   sending to a customer from a limited use credit card number issuer a limited use credit card number which is not yet activated;

   receiving acknowledgment of delivery by the customer of the limited use credit card number which is not yet activated;

   communicating with a limited use card number card issuer to activate the limited use credit card number before it can be used in a transaction; and

   validating the limited use credit card number to have associated limited use properties.

2. The method of claim 1 wherein said limited use properties are one or more properties selected from a group consisting of: a specific time period, a specific merchant, a specific group of merchants, a specific type of transaction, and a specific number of transactions.

3. The method of claim 1 or 2 wherein said sending step includes sending to the customer a software package from the card issuer along with a unique personal validity limited credit card number, said software package facilitating completion of the merchants web page.

4. The method of any preceding claim wherein said validation step includes:

activating validity limited credit card software using a user identification to identify the user with the card issuer;

requesting validation of a limited use credit card for a merchant as identified by a merchant identification number; and

providing an opinion for a user to specify additional limitations other than the specific merchant to the limitation on the limited use credit card number.

5. The method as claimed in any preceding claim further comprising the steps of:

receiving by a merchant a limited use credit card number;

processing by a merchant the received limited use credit card number in a transaction as any other credit card number;

passing the transaction through to the card issuer's processing system;

requesting authorization of the transaction at the card issuer's processing system against the associated limited use properties; and

deactivating the limited use credit card number by the card issuer when a use-triggered condition is present.

6. The method as claimed in any preceding claim further comprising the steps of:

deactivating the limited use credit card number by the card issuer when a use-triggered condition is present;

communicating with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating step; and

revalidating the limited use credit card number with associated limited use properties.

7. The method as claimed in any preceding claim wherein the limited use properties of the revalidated limited use credit card number are different from the limited use properties of the validated limited use credit card number.

8. A method of conducting a limited use credit card transaction in a financial transaction system capable of using at least one limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of the at least one credit card number comprising the steps of:

initiating a transaction by a customer presenting a limited use credit card number to a merchant;

routing said limited use credit card number to a central processing system; and

determining whether said limited use credit card number has been deactivated because at least one use-triggered condition has been satisfied.

9. The method of claim 8, wherein the limited credit card number is linked to an organization selected from a group consisting of: a utility, a public network service provider, a telephone company, a bank account, a prepaid account and a credit card issuer.

10. The method of claim 8 or 9 further comprising

transmitting a signal to the organization which is linked to the limited use credit card number, the signal including original transaction details if the limited use credit card number has not been deactivated;

performing a credit check on the user to determine whether authorization can be obtained against the limited use credit card number; and

transmitting a signal to the merchant with the results of the authorization determining step for the limited use credit card number.

11. The method of any of claims 8 to 10 wherein the use-triggered conditions include one or more conditions selected from a group consisting of: a specific time period, a specific merchant, a specific group of merchants, a specific type of transaction, and a specific number of transactions.

12. The method of any of claims 8 to 11 further comprising transmitting a signal to the merchant denying authorization of the card number if the credit card number has been deactivated.

13. The method of any of claims 8 to 12, wherein the limited use credit card number is associated with a master credit card number, further comprising:

transmitting a signal to a master credit card issuing facility which issued the limited use credit card number, the signal including original transaction details but with the limited use credit card number remapped to be a master credit card number if the limited use credit card number has not been deactivated;

determining whether authorization can be obtained against the master credit card number;

remapping the results of the authorization determining step to the limited use credit card number for transmission to the merchant; and

transmitting a signal to the merchant with the results of the authorization determining step for the limited use credit card number.

14. The method of claim 13, further comprising authorizing the transaction based on the results of the authorization determining step.

15. The method of claim 13, further comprising declining authorization of the transaction based on the results of the authorization determining step.

16. A method of conducting a settlement in a financial transaction system capable of using at least one limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of the at least one credit card number and which is associated the master account number of a customer comprising the steps of:

transmitting a signal from a merchant to a central processing system according to leading digits of the limited use card number;

remapping the limited use credit card number with the master credit card number;

transmitting said remapped master credit card number to issuer processing facility which issued the master credit card number;

settling the transaction by payment, if appropriate, to the central processing system;

remapping the master credit card number back to the limited use credit

card number; and

transmitting the limited use credit card number and payment information, if appropriate, to the merchant.

17. The method of claim 16, wherein the use-triggered conditions include one or more conditions selected from a group consisting of: a specific time period, a specific merchant, a specific group of merchants, a specific type of transaction, and a specific number of transactions.

18. A method of providing remote access devices for accessing limited use numbers in a financial transaction system capable of using at least one limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of the at least one credit card number and which is associated the master account number of a customer comprising the steps of:

submitting user authentication information and the master account number for entry into a database;

determining whether the user is a valid user of the master credit card number;

registering the user if the user if determined to be a valid user; and

obtaining, by registered user, a software package to which enables communication with a remote access device support server to enable the issuance of limited use card numbers.

19. The method of claim 18 wherein the use-triggered conditions include one or more conditions selected from a group consisting of: a specific time period, a specific merchant, a specific group of merchants, a specific type of transaction,

and a specific number of transactions.

20. The method of claim 18 or 19 further comprising:

using the software package to initiate communication with the remote access support server;

authenticating the user at the remote access support server;

requesting a limited use number by an authenticated user;

obtaining an available limited use number;

entering the limited use number and the specified limitations into the database such that the limited use number is associated with the user's information already in database; and

transmitting the limited use number to the user.

21. The method of any of claims 18 to 20, further comprising: specifying by the authenticated user any additional transaction limitations desired.

Fig. 1

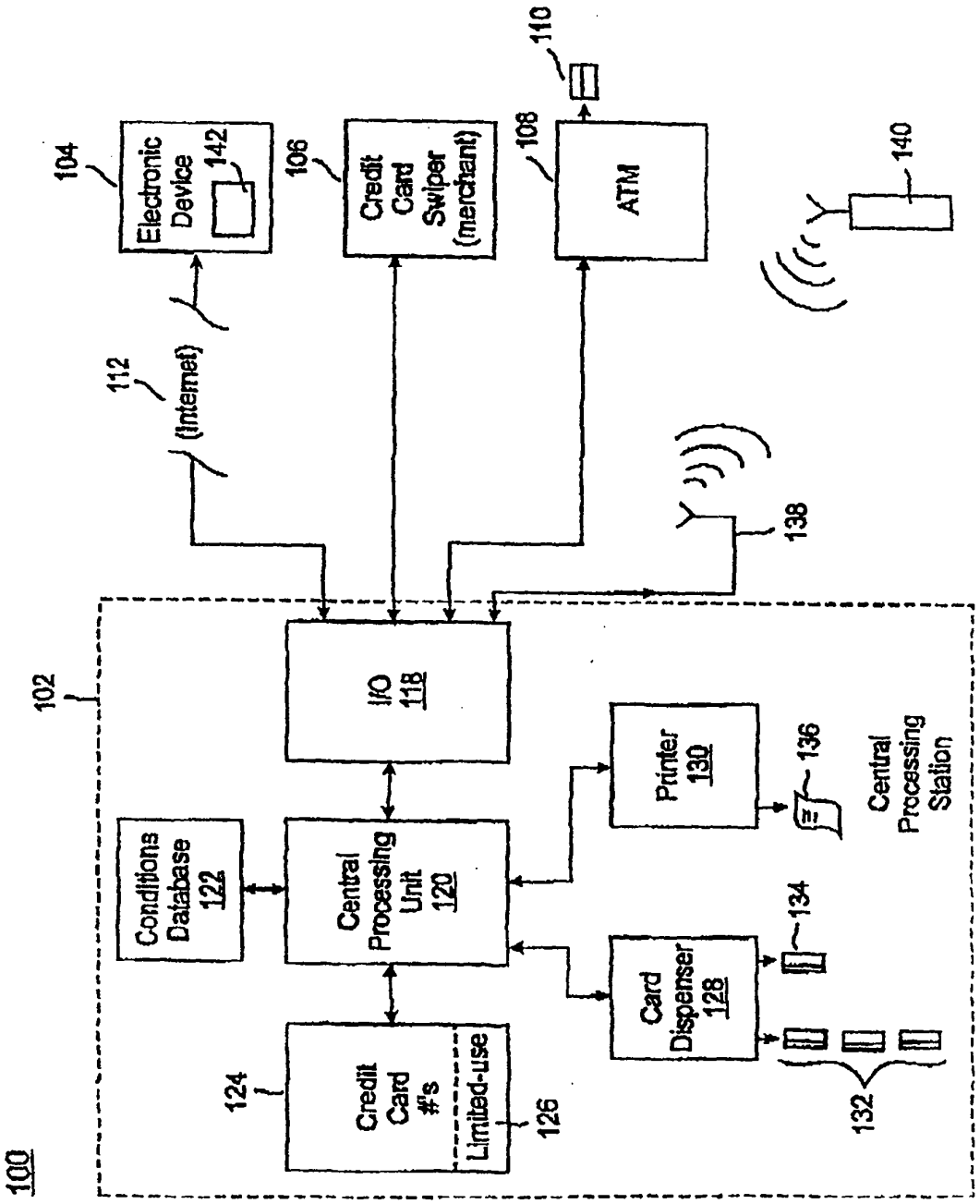

100
102
104
Electronic Device
142
106
Credit Card Swiper (merchant)
108
ATM
110
112
(Internet)
140
138
I/O 118
Printer 130
136
Central Processing Station
Conditions Database 122
Central Processing Unit 120
Card Dispenser 128
134
Credit Card #'s
Limited-use
124
126
132

Fig. 2

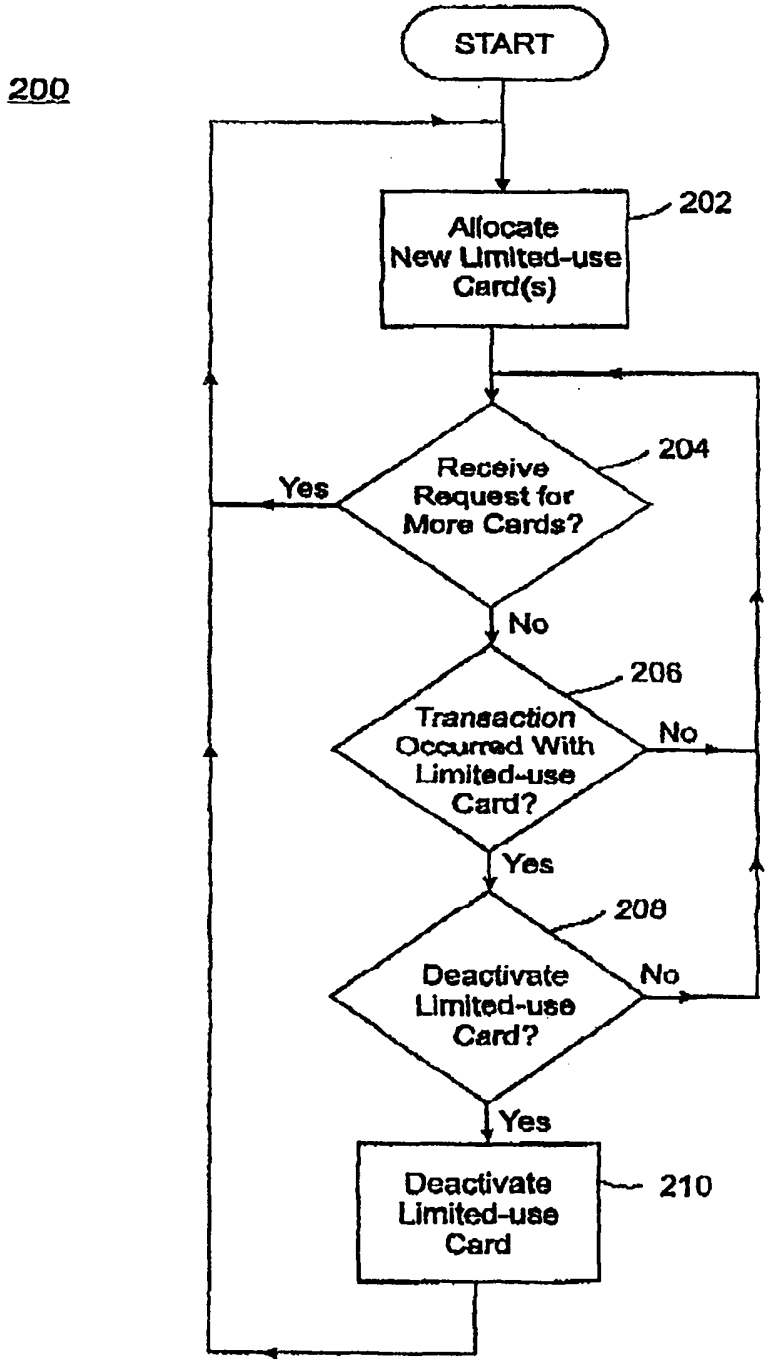

200
START
Allocate New Limited-use Card(s)
202
Receive Request for More Cards?
204
Yes
No
Transaction Occurred With Limited-use Card?
206
No
Yes
Deactivate Limited-use Card?
208
No
Yes
Deactivate Limited-use Card
210

Fig. 3

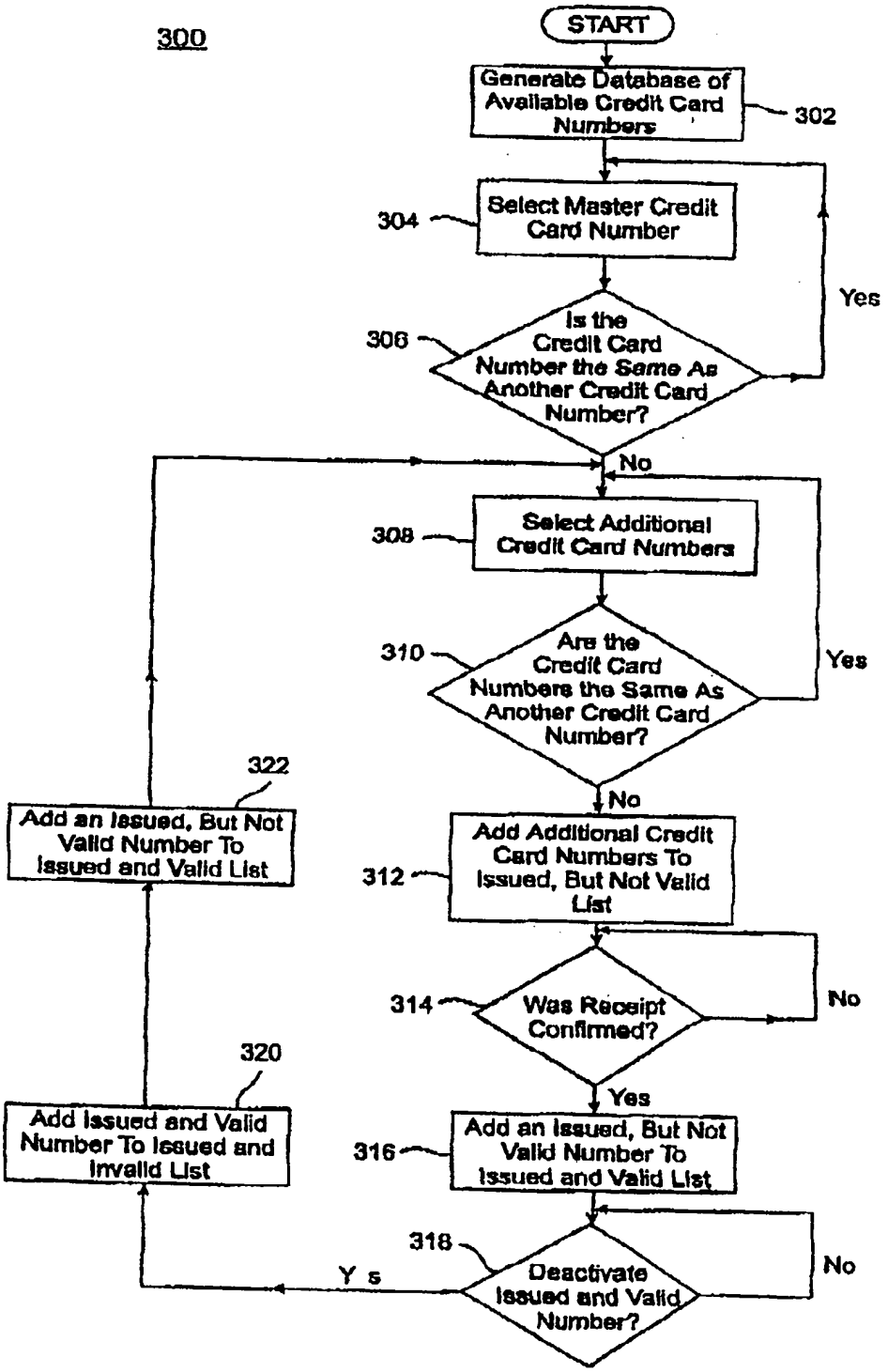

300
START
Generate Database of Available Credit Card Numbers
302
Select Master Credit Card Number
304
Is the Credit Card Number the Same As Another Credit Card Number?
306
Yes
No
Select Additional Credit Card Numbers
308
Are the Credit Card Numbers the Same As Another Credit Card Number?
310
Yes
No
Add Additional Credit Card Numbers To Issued, But Not Valid List
312
Was Receipt Confirmed?
314
No
Yes
Add an Issued, But Not Valid Number To Issued and Valid List
316
Deactivate Issued and Valid Number?
318
No
Yes
Add Issued and Valid Number To Issued and Invalid List
320
Add an Issued, But Not Valid Number To Issued and Valid List
322

Fig. 4

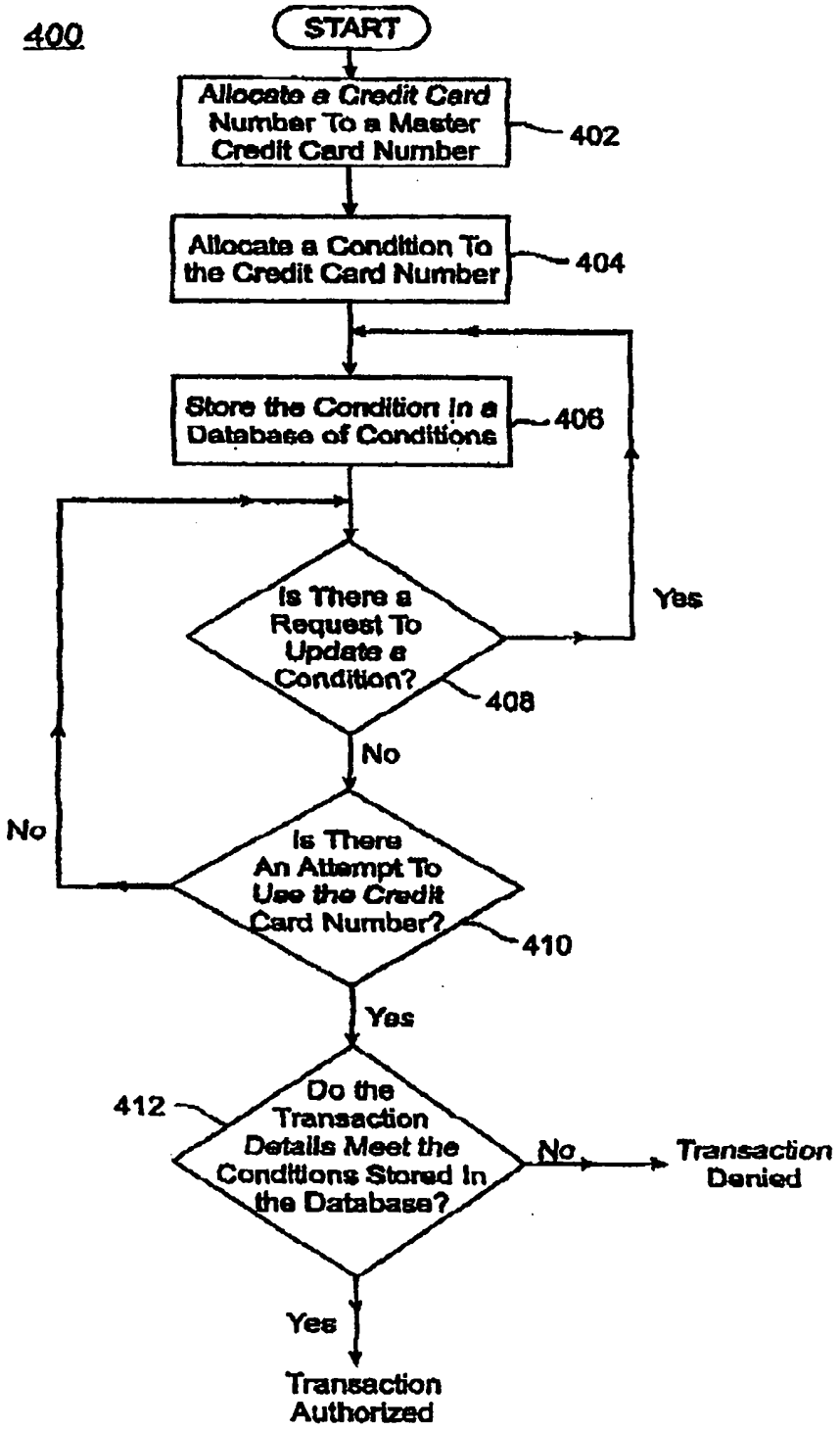

400
START
Allocate a Credit Card Number To a Master Credit Card Number
402
Allocate a Condition To the Credit Card Number
404
Store the Condition In a Database of Conditions
406
Is There a Request To Update a Condition?
408
Yes
No
Is There An Attempt To Use the Credit Card Number?
410
No
Yes
412
Do the Transaction Details Meet the Conditions Stored In the Database?
No
Transaction Denied
Yes
Transaction Authorized

Fig. 5

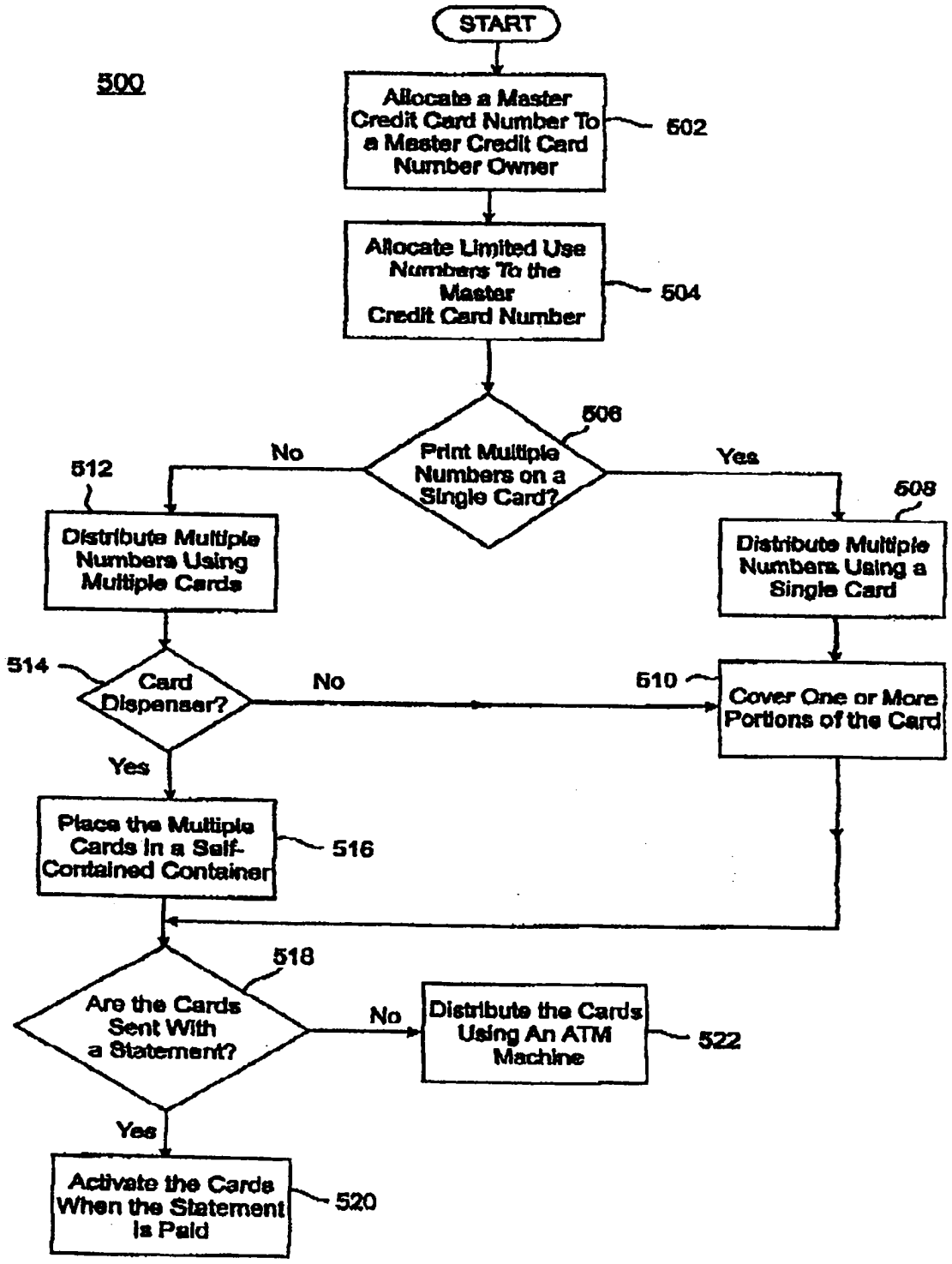

500
START
Allocate a Master Credit Card Number To a Master Credit Card Number Owner
502
Allocate Limited Use Numbers To the Master Credit Card Number
504
Print Multiple Numbers on a Single Card?
506
No
Yes
512
Distribute Multiple Numbers Using Multiple Cards
508
Distribute Multiple Numbers Using a Single Card
514
Card Dispenser?
No
510
Cover One or More Portions of the Card
Yes
Place the Multiple Cards In a Self-Contained Container
516
518
Are the Cards Sent With a Statement?
No
Distribute the Cards Using An ATM Machine
522
Yes
Activate the Cards When the Statement Is Paid
520

Fig. 6

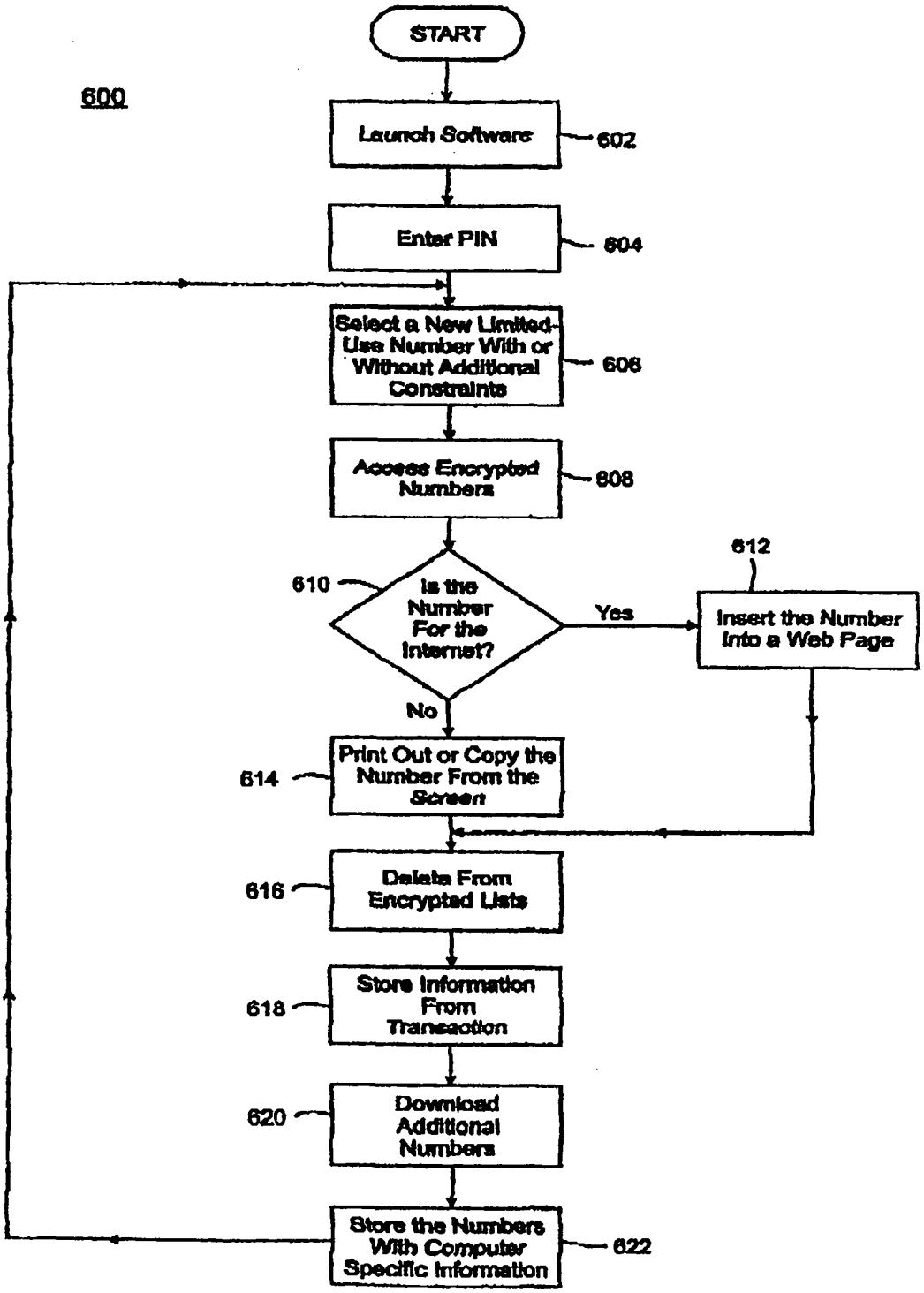

600
START
Launch Software
602
Enter PIN
604
Select a New Limited-Use Number With or Without Additional Constraints
606
Access Encrypted Numbers
608
610
Is the Number For the Internet?
Yes
612
Insert the Number Into a Web Page
No
614
Print Out or Copy the Number From the Screen
616
Delete From Encrypted Lists
618
Store Information From Transaction
620
Download Additional Numbers
Store the Numbers With Computer Specific Information
622

Fig. 7

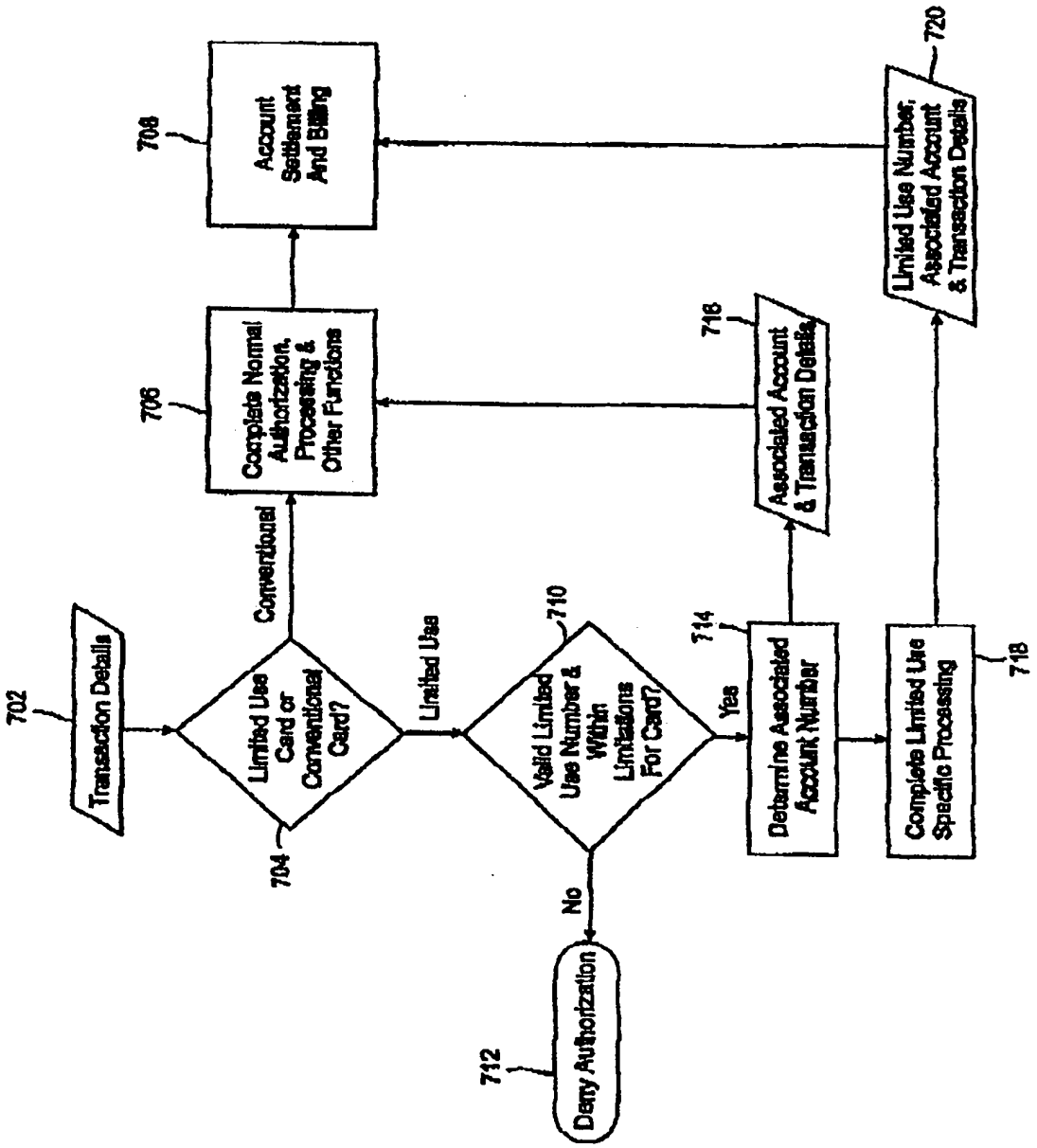

Transaction Details
702
Limited Use Card or Conventional Card?
704
Conventional
Limited Use
Complete Normal Authorization, Processing & Other Functions
706
Account Settlement And Billing
708
Valid Limited Use Number & Within Limitations For Card?
710
No
Deny Authorization
712
Yes
Determine Associated Account Number
714
Associated Account & Transaction Details
716
Complete Limited Use Specific Processing
718
Limited Use Number, Associated Account & Transaction Details
720

Fig. 8

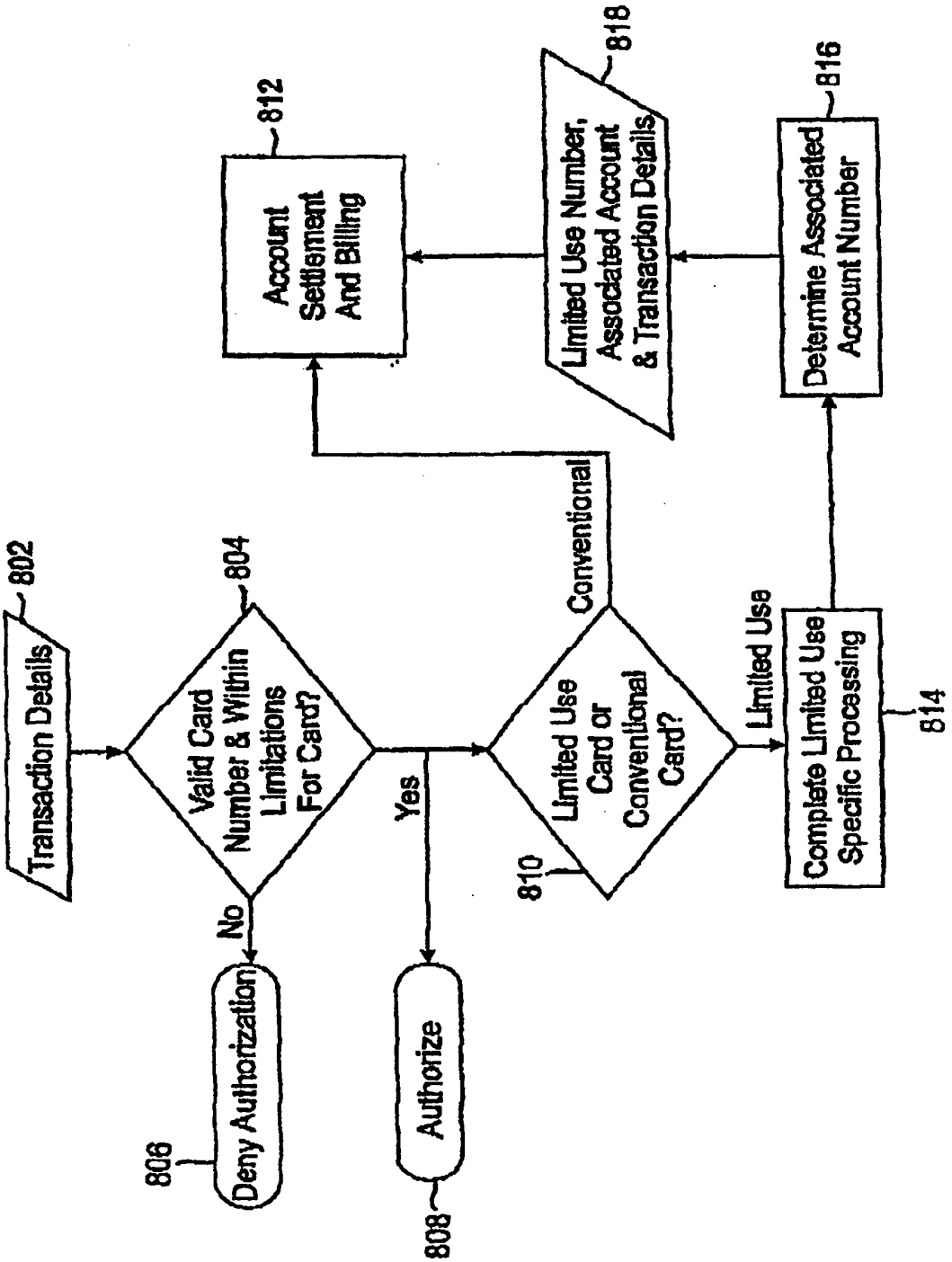

802
Transaction Details
804
Valid Card Number & Within Limitations For Card?
No
806
Deny Authorization
Yes
808
Authorize
Conventional
810
Limited Use Card or Conventional Card?
Limited Use
812
Account Settlement And Billing
818
Limited Use Number, Associated Account & Transaction Details
816
Determine Associated Account Number
814
Complete Limited Use Specific Processing

FIG. 9

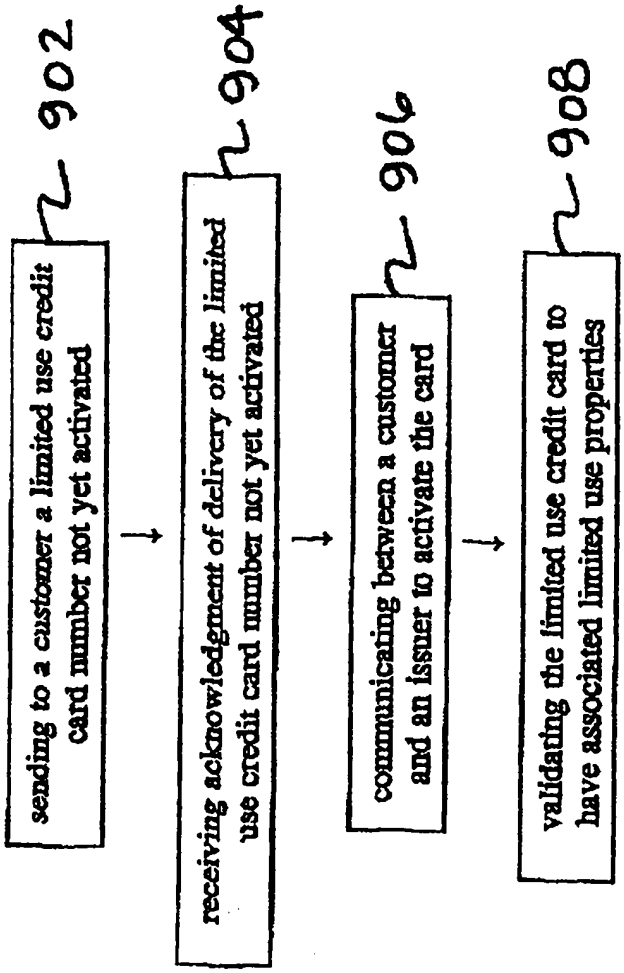
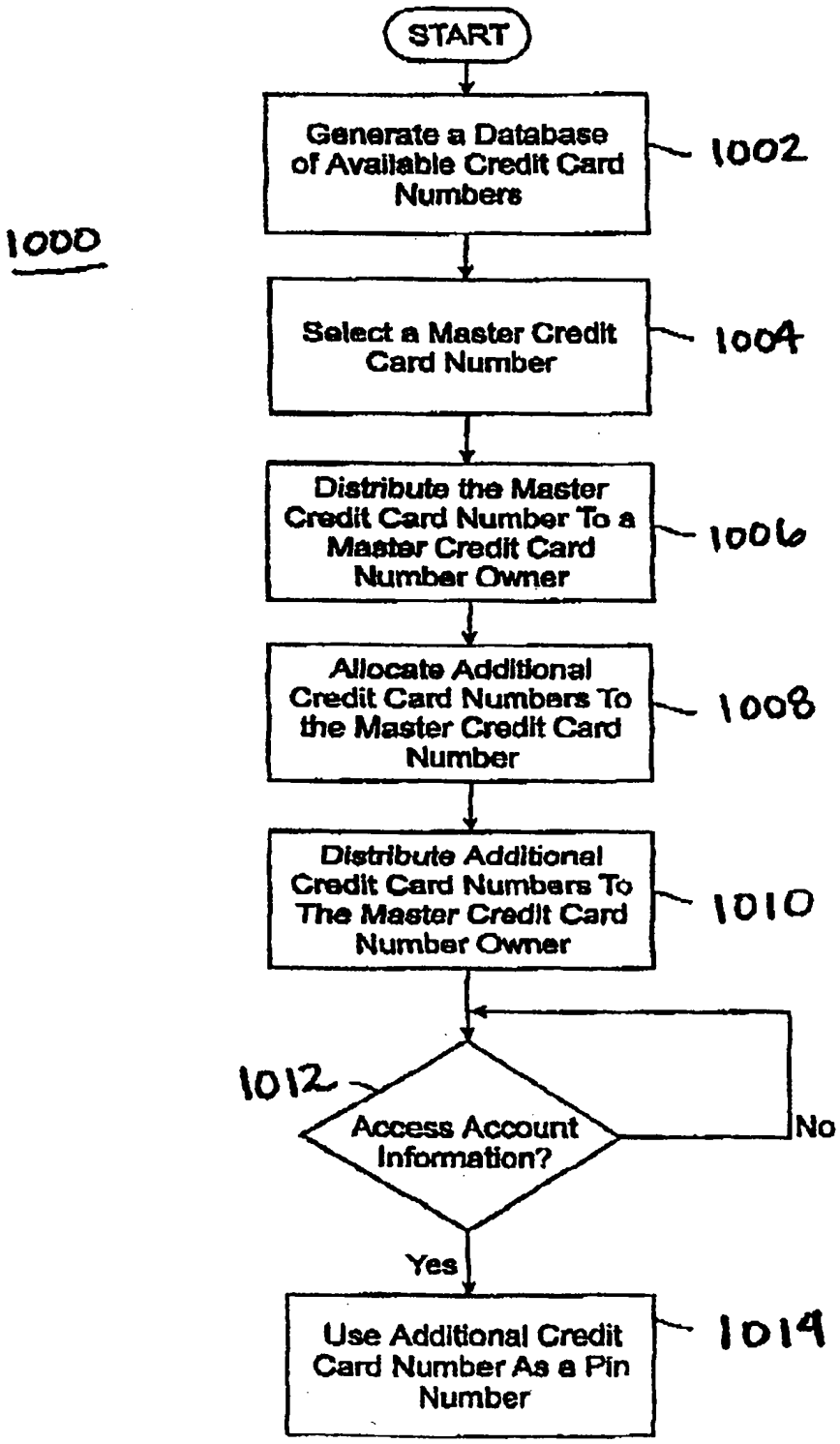

902
sending to a customer a limited use credit card number not yet activated
904
receiving acknowledgment of delivery of the limited use credit card number not yet activated
906
communicating between a customer and an issuer to activate the card
908
validating the limited use credit card to have associated limited use properties

FIG. 10


1000
START
Generate a Database of Available Credit Card Numbers
1002
Select a Master Credit Card Number
1004
Distribute the Master Credit Card Number To a Master Credit Card Number Owner
1006
Allocate Additional Credit Card Numbers To the Master Credit Card Number
1008
Distribute Additional Credit Card Numbers To The Master Credit Card Number Owner
1010
1012
Access Account Information?
No
Yes
Use Additional Credit Card Number As a Pin Number
1014

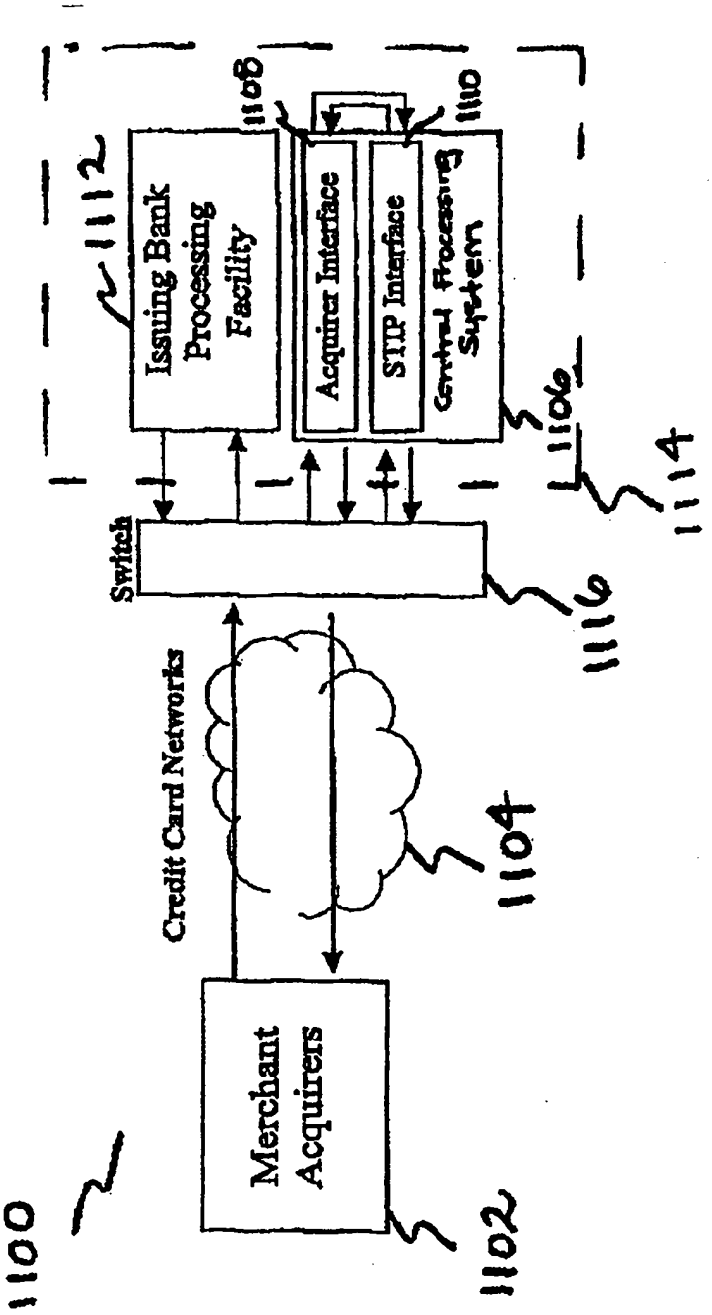

1100
1102
Merchant Acquirers
Credit Card Networks
1104
Switch
1116
1114
1106
Issuing Bank Processing Facility
1112
Acquirer Interface
STIP Interface
Central Processing System
1108
1110

FIG. 11

FIG. 12

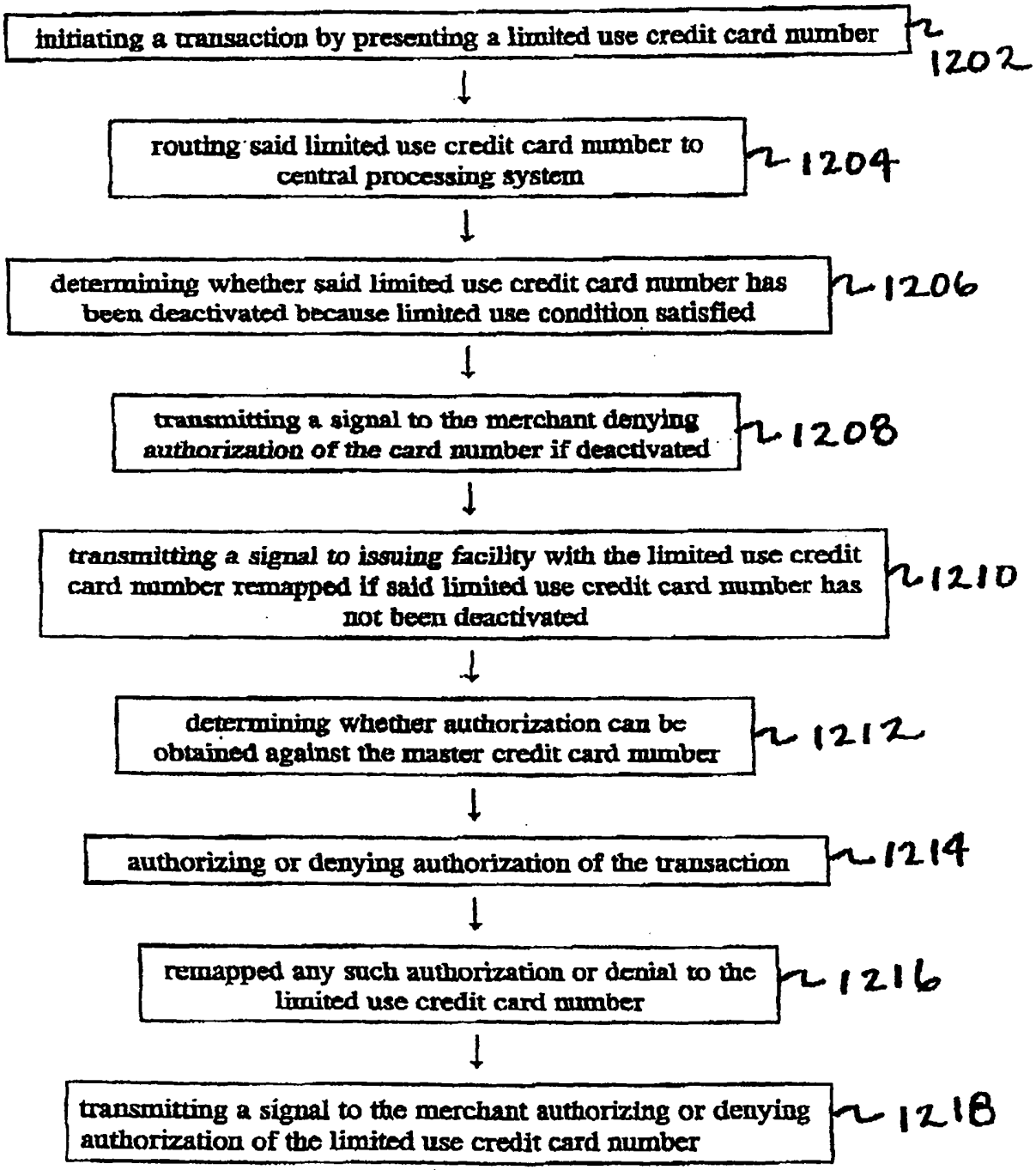
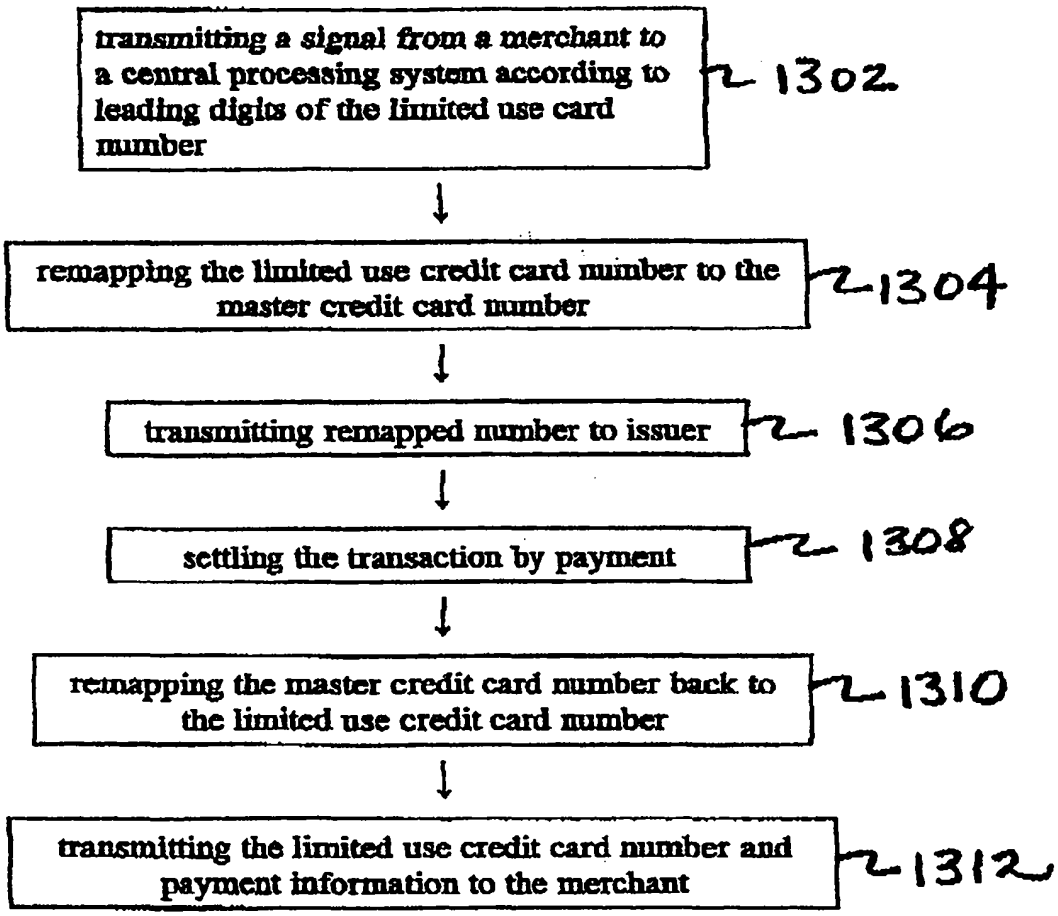

initiating a transaction by presenting a limited use credit card number
1202
routing said limited use credit card number to central processing system
1204
determining whether said limited use credit card number has been deactivated because limited use condition satisfied
1206
transmitting a signal to the merchant denying authorization of the card number if deactivated
1208
transmitting a signal to issuing facility with the limited use credit card number remapped if said limited use credit card number has not been deactivated
1210
determining whether authorization can be obtained against the master credit card number
1212
authorizing or denying authorization of the transaction
1214
remapped any such authorization or denial to the limited use credit card number
1216
transmitting a signal to the merchant authorizing or denying authorization of the limited use credit card number
1218

FIG. 13


transmitting a signal from a merchant to a central processing system according to leading digits of the limited use card number
1302
remapping the limited use credit card number to the master credit card number
1304
transmitting remapped number to issuer
1306
settling the transaction by payment
1308
remapping the master credit card number back to the limited use credit card number
1310
transmitting the limited use credit card number and payment information to the merchant
1312

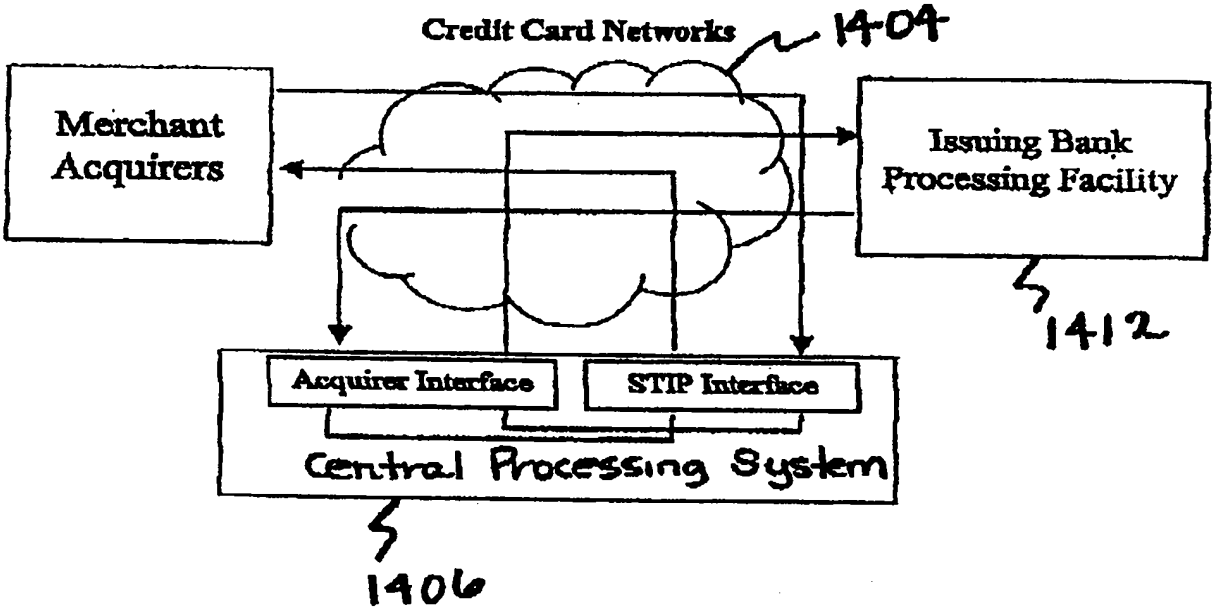

Credit Card Networks
1404
Merchant Acquirers
Issuing Bank Processing Facility
1412
Acquirer Interface
STIP Interface
Central Processing System
1406

Fig. 14

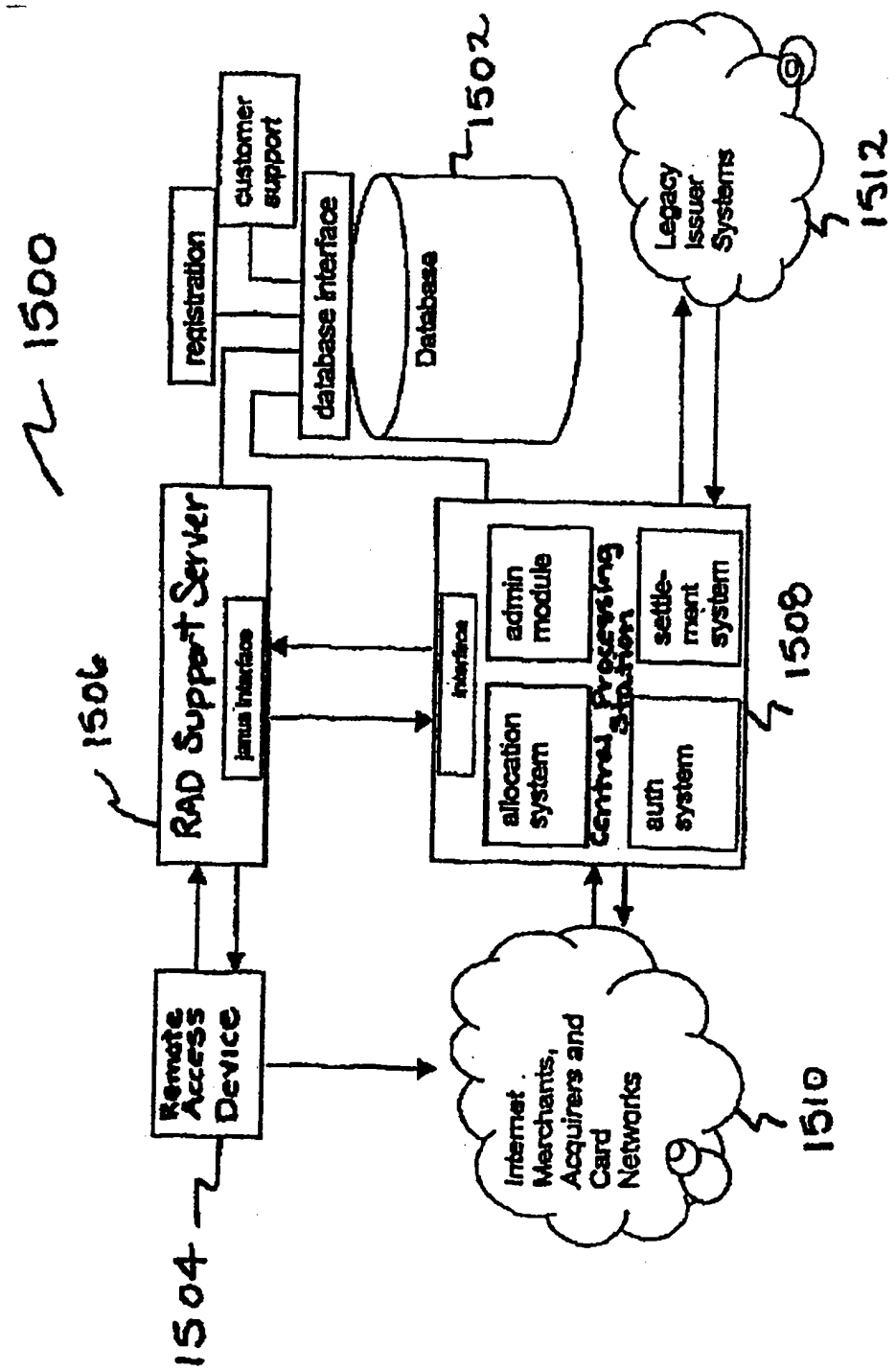
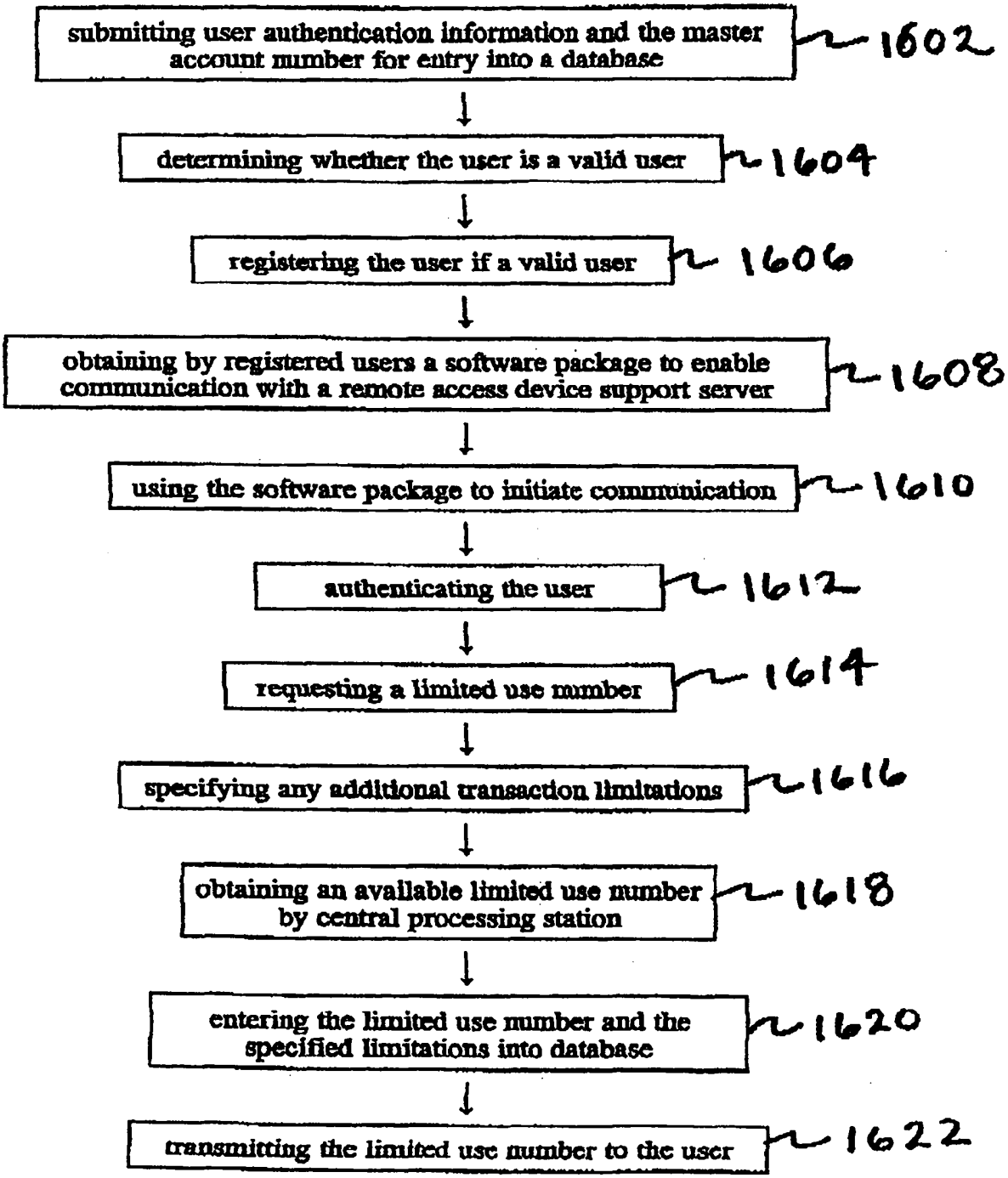

1500
1502
Database
registration
customer support
database interface
Legacy Issuer Systems
1512
RAD Support Server
1506
janus interface
interface
admin module
settle-ment system
allocation system
Central Processing System
auth system
1508
Remote Access Device
1504
Internet Merchants, Acquirers and Card Networks
1510

FIG. 15

FIG. 16


submitting user authentication information and the master account number for entry into a database
1602
determining whether the user is a valid user
1604
registering the user if a valid user
1606
obtaining by registered users a software package to enable communication with a remote access device support server
1608
using the software package to initiate communication
1610
authenticating the user
1612
requesting a limited use number
1614
specifying any additional transaction limitations
1616
obtaining an available limited use number by central processing station
1618
entering the limited use number and the specified limitations into database
1620
transmitting the limited use number to the user
1622

INTERNATIONAL SEARCH REPORT

In ational Application No
PCT/IE 00/00025

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	WO 98 30985 A (AEROTEL) 16 July 1998 (1998-07-16) the whole document	1,2,8,9, 18,19 3-5, 10-15,20
Y	US 5 777 305 A (M. BROOKS SMITH) 7 July 1998 (1998-07-07) abstract; claims; figures	1,2,8,9, 18,19
A	GB 2 305 393 A (POWERHOUSE MARKETING) 9 April 1997 (1997-04-09) the whole document	1,2,6,8, 9,18,19
A	EP 0 590 861 A (AT & T) 6 April 1994 (1994-04-06) abstract; claims; figures column 3, line 15 - line 42	1-5, 8-15, 18-20

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 May 2000	02/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IE 00/00025

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	WO 97 19549 A (AVERY DENNISON) 29 May 1997 (1997-05-29) abstract; claims; figures page 7, line 26 -page 8, line 29	1-21
A	US 5 868 236 A (D.G. RADEMACHER) 9 February 1999 (1999-02-09)	
A	US 5 696 908 A (K. MUEHLBERGER) 9 December 1997 (1997-12-09)	
A	US 4 725 719 A (J.E. ONCKEN) 16 February 1988 (1988-02-16)	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int ational Application No
PCT/IE 00/00025

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9830985 A	16-07-1998	EP 0988623 A	29-03-2000
US 5777305 A	07-07-1998	NONE	
GB 2305393 A	09-04-1997	NONE	
EP 0590861 A	06-04-1994	CA 2100134 A	30-03-1994
		JP 7129671 A	19-05-1995
		MX 9305830 A	30-06-1994
		US 5485510 A	16-01-1996
WO 9719549 A	29-05-1997	US 5673309 A	30-09-1997
		AU 7738196 A	11-06-1997
US 5868236 A	09-02-1999	NONE	
US 5696908 A	09-12-1997	NONE	
US 4725719 A	16-02-1988	NONE	